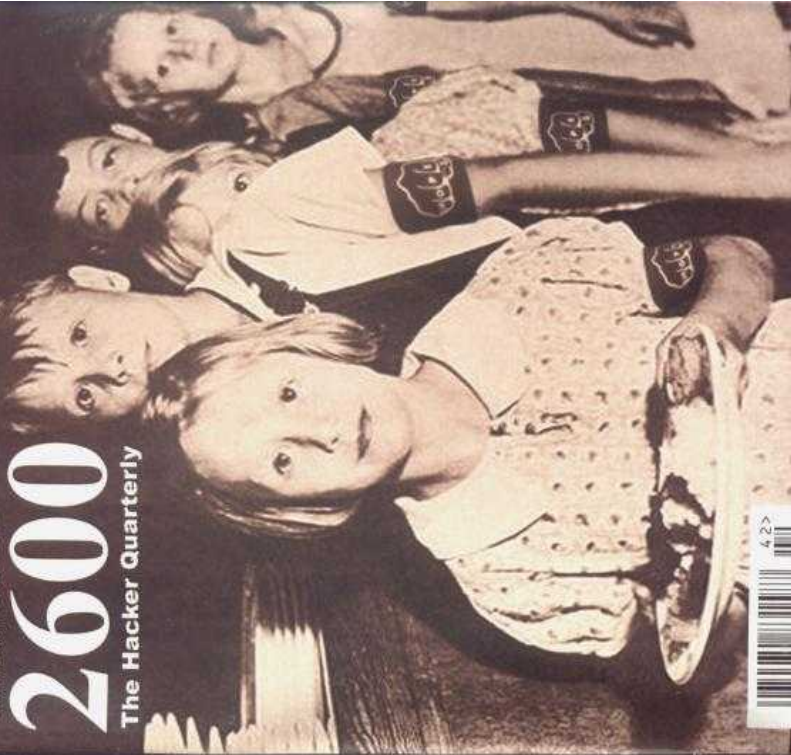


Volume Twenty-One, Number Two  
Summer 2004, \$5.50 US, \$8.15 CAN

**2600**  
The Hacker Quarterly



**Are your CHILDREN  
IN line or ON line?**

# Bulgarian Payphones



All of these photos were taken in Sofia. Here we see a modern orange coin and card phone.



And when a phone only takes cards, they appear to simply cut the bottom half off.



Here's a blue card phone, which was right next to the orange phone above. Such spectacular displays of color are virtually unheard of here in the States.



The old style payphone with funky surrounding. Drab, yet intriguing.

*Photos by kamivOre*

Look on the other side of this page for even more photos!

"Men are only as good as their technical development allows them to be."  
- George Orwell

**STAFF**

**Editor-In-Chief**  
Emmanuel Goldstein

**Layout and Design**  
Shapeshifter

**Cover Design**  
Dabu Ch'wald

**Office Manager**  
Tampur

**Writers:** Bernie S., Billisf, Bland Inquisitor, Eric Corley, Dalai, Dragon, John Drake, Paul Estey, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Milnick, The Prophet, David Ruderman, Screamer Chaotix, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

**Webmasters:** Julintz, Kerry

**Network Operations:** css, mtc

**Broadcast Coordinators:** Julintz, Pete, daRonin, Digital Mercenary, Kobold, W3rd, Gehenna, Britton, Jee, Logix, Pyey, Mighty Industries, DJ Riz, Dave

**IRC Admins:** daRonin, Digital Mercenary, Shardy, The Electronic Delinquent

**Inspirational Music:** Manu Chao, Phil Ochs, Combustible Edison, Sparks, Philip Glass, 386DX

**Shout Outs:** Woz, Kdm, Jello, Dan Morgan, Visual Goodness, Lazlow, Cheshire, Adrian

2600 ISSN# 10749-8851 Published quarterly by 2600 Enterprises, Inc. 2 Fawcett St. Ithaca, NY 14850

Periodicals postage paid at Ithaca, NY and additional mailing offices

**POSTMASTER:**

Send address changes to:  
2600 PO Box 522  
Middle Island, NY 11953-0522  
Copyright © 2002  
2600 Enterprises, Inc.

**YEARLY SUBSCRIPTION:**

U.S. and Canada:  
\$20 individual, \$30 corporate, U.S. funds Overseas: \$30 individual, \$45 corporate.  
Back issues available for purchase at \$20 per year, \$26 per year overseas.  
Individual issues available from 1988 on at \$5.00 each, \$6.50 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**

2600 Subscription Dept., PO Box 522  
Middle Island, NY 11953-0522  
tsubs@2600.com

**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**

2600 Editorial Dept., PO Box 909  
Middle Island, NY 11953-0909  
tedit@2600.com, article@2600.com  
2600 Office Line: 631-751-2600  
2600 FAX Line: 631-474-2677

 **Shockers** 

Mirroring the Future 4

Scumware, Spyware, Adware, Sneakware 6

ClearChannel's Dirty Little Secret 10

Impromptu Lock Picks 12

Magstripe Interfacing - A Lost Art 15

Listening Via Linux 20

Passwords on a Cue Cat 22

The Global Date Format 22

Behind the Scenes of ITEC and the Milwaukee Bus System 24

Omni Locks and Stupid Politics 25

A Guide to Internet Piracy 26

Letters 30

Consumer Spookware vs. Your Castle 40

A Lesson on Trust 45

Fun With Netcat 52

The Lantrox SCS 1b20: An Unpublicized Gold Mine 54

Marketplace 56

Meetings 5A

# Mirroring the Future

When this issue is released, our fifth conference will have been held in New York City. We named it, fittingly, The Fifth HOPE. For those unfamiliar, HOPE is an acronym for Hackers On Planet Earth. This also marks the tenth anniversary of the first HOPE conference in 1994, the first time ever that hackers gathered in such large numbers in the United States. And of course, we're also in the midst of our 20th anniversary here at 2600, founded somewhat ironically in 1984.

We see a certain symmetry in all of these events and anniversaries. But more importantly, we see symmetry in the goals and ideals expressed every day in the hacker community as they relate to those of the human race in the 21st century. The things we see as important, the technology we find ourselves playing with and designing, the limits we constantly test and push, and the freedoms we instinctively stand up for - these are all being mirrored in the "real" world on a daily basis.

Most of us never intended for things to become so serious, much like we never intended for this publication to be of interest to more than a very narrow portion of the populace. To this day, hackers are born out of the curiosity that relatively few people feel towards technology and they move forward through the determination of wanting to figure something out or make it work better. That's really all it is and all it has ever been. No pressing desire to change the world, no compelling need to be the focal point of the media, and certainly no wish to be fashionable. Events, however, have an odd way of changing one's focus and altering the path.

Anyone who could have predicted the explosion of technology in the past 20 years could have also predicted the social consequences and commandments that came along with it. Obviously when everyone gains the ability to operate the equivalent of a printing

press via the Internet, authority figures everywhere will start to clamp down on what can be said and how. When digital technology allows perfect copies of audio and video to be created and shared, the status quo is going to be threatened and panic will ensue. When computers and databases become more and more integrated, our private information will be shared by more and more entities. And it will become increasingly difficult to remain anonymous as we move closer to a society that demands accountability for one's every move, purchase, and transgression.

Every one of these issues is of great concern to the vast majority of people in our present society. Suddenly the technology that made us curious - and got many of us labeled as weird for taking such an abnormal interest in it - is changing the very nature of the world. And to those people who didn't take an interest before, a lot of these sudden changes and all-encompassing issues are extremely disconcerting. They are to us as well, although anyone paying attention would know that the changes were anything but sudden. They are part of a pattern, one which is continuing and one which will only grow worse in time, so long as people remain ignorant and convinced that they lack both the intellect and ability to do anything about it.

As we well know, that is one of the greatest weapons any agent of oppression can possess: the ability to convince people that they can't make a difference and that certain things are inevitable. We're here to tell you that *anyone* can make a difference and *nothing* is a certainty. With that in mind, now is as good a time as any to take a look at the developments going on around us and decide if that is really the direction we want to be heading in.

Why does this responsibility fall upon the hacker community in particular? Two reasons. We understand how a lot of the technology used to implement these changes really works. Which means we know the weaknesses and the potential abuses from both outside and within. And we also have a history of standing up to authority - whether it's the authority that tells us not to ask questions or the authority that locks us away in prison for using technology in a way that wasn't quite authorized.

The hacker spirit has proven very difficult to crush over the years. Even if one voice is silenced for revealing information, another will soon take its place. No matter what the restrictions or penalties surrounding a particular bit of technology, you can bet that hackers somewhere are figuring out ways to defeat it in the public arena. It's just that now there are a great many more people paying attention to the results.


Hacking has never been as relevant and as important as it is today. While many of us are still kids playing with toys and experiment-

ing, there's a whole other aspect that the entire world is watching. If our privacy is at risk, our safety is in danger, or our rights are gradually being extinguished, odds are the abuse of technology plays some part in this. Ironically, hackers are frequently viewed in the mainstream as the ones who abuse high tech. But even those subscribing to this notion can see the logic of paying attention to what hackers uncover. To ignore this is to walk blindly into unknown territory.

So we find ourselves in a very different world than when we started in 1984 or even when we held the first HOPE conference a decade ago. We've become far more dependent on technology for nearly every aspect of our lives and technology is being used intrusively on a steadily increasing basis. If we have the expertise to uncover information on how it all works, then we also have the obligation to our fellow citizens to make it all public. Twenty years from now, the world will be a very different place. We have the ability to educate others and influence the changes that transpire along the way.

## At Long Last The Wait Is Over!

Years in the making, the **FREEDOM DOWNTIME DVD** is now complete. We think you'll be pleased. Included in this two disc set:  
 Freedom Downtime  
 Kevin Mitnick Interview  
 Nearly 3 hours of lost footage, extra scenes, interviews, the trailer, outtakes, and more  
 20 language translations (no kidding)  
 Commentary track  
 Surprises and special features (trust us)



If you can find a DVD with more going on, let us know about it. No region coding, no copy protection. These discs will play anywhere. The double disc set is yours for \$30. (Freedom Downtime videos (VHS/VHS) are still available for \$15.)

Freedom Downtime  
 c/o 2600  
 PO Box 752  
 Middle Island, NY 11953  
 USA

Or order from our online store at  
<http://Store.2600.com>

# Scumware, Spyware, Adware,



## SNEAKWARE

by shinohara  
shinohara@zip.jp.com

Forget about cookies. They're child's play compared to the sheer nastiness of Gator or to the insolence of Newton Knows Best. The more I studied them, the angrier I got. I simply had to write an article about them to warn people.

### What is Spyware and Adware?

Let's first get our definitions straight. There are a lot of different names floating around. Spyware is seemingly useful software installed on your PC that will observe your actions, gather data on your surfing habits and what you are interested in, compile that data, and send it back to the main server. In this sense, it's similar to a Trojan horse. Adware mainly receives ads in the form of images (simple gifs, animated gifs) or other multimedia type files. Adware can also include components which will spy on users' actions. Those components which are installed on the PC without a user's permission can be called sneakyware. Spamware is essentially the same as adware - serving unwanted ads. A lot of people (myself included) have begun calling all of these types simply scumware.

### Gator

There are many scumwares on the market that we can examine. In fact, if we try to look at all of them, we will spend literally days doing so. That is why I have narrowed the list to the most notorious ones and the ones you are most likely to meet. Gator/GAIN is one of them.

Gator is one of the nastiest pieces of spyware around. Gator's parent company changed their name to Clara Corporation (<http://www.clara.com>) in an attempt to disassociate themselves from Gator. But they still sink just as bad. It is carried by almost all P2P file-share apps as well as free ISPs, like Netzero. In fact I can't seem to be able to get rid of it. Every time I turn around, there is a fresh install of Gator on my system. Worse, Gator software is composed of several separate modules, incarnations, and names: Gator,

OfferCompanion, Trickler, GAIN, GMT.exe, CMESys.exe, and a quite a few others. Gator/GAIN is marketed as a software product that will automatically fill in passwords and other form-elements on web pages, but its main purpose is to load an advertising spyware module called OfferCompanion which displays pop-up ads when visiting some websites. Once installed, Gator's software never stops running and it monitors pretty much everything a user does. The program is freely distributed by <http://www.gainpublishing.com> but it can be found in a slew of file-sharing applications, including the "most-downloaded software" on the Internet - the new Kazaa version that just came out a few days ago and which I investigated while writing this article. In fact, you cannot even install and use Kazaa without agreeing to also install Gator. Talk about asshole!

Gator are so insolent that they justify what they do as "right." From a CNET news.com article in 2001: "We get lots of angry calls; maybe even an attorney calls up because they're angry," said Gator's Eagle. "We explain it's the consumer's right because we're invited onto the desktop. We're not changing their content; we're popping up on the consumer's desktop. Don't they advertise on TV showing competitor comparisons? The only difference is that we're more effective. The next call we get is usually from the VP of sales, saying, 'We would like to work with you.'"

### How Do You Get Infected With It?

In Gator's case, it can come into your PC in three ways: either pre-bundled in a file-sharing program such as Kazaa, iMesh and a few others; in some alleged "freeware" such as AudioGalaxy, GoZilla, and Weatherbug, or the so-called drive-by-installation, using Internet Explorer's ActiveX controls where a website attempts to download and install software (executable code) from a banner or a pop-up ad on the user's PC. This is by far the sneakiest way, since most average users don't have a clue about Secure Zone settings and

often choose Yes when confronted with a dialog, thinking the browser is simply installing a needed plug-in for a website they're viewing. Depending on the browser's security settings, the software will either download silently and without any user action, or present an install dialog.

Gator is also now available for download in separate freeware applications called eWallet and Precision Time/Date Manager; but nobody in their right mind would even use those. When installed, Gator begins to slowly download and install other modules.

### What Does It Do?

Gator has two main purposes: to deliver ads to the user based on the profile it builds and to collect information on the user's habits, including (but not limited to) every page visited, the length of time the user spent at each site, what the user is interested in, what ads (if any) the user clicks on, any special searches the user does, any keywords entered, and any files downloaded. It saves all of that info in a file on your computer which identifies your PC through its IP address.

The newest Gator trick is to hijack a pop-up ad from another company when users visit a competitor's website. This practice (which I find rather amusing; I must admit) is known as "being Gatored." It is accomplished by selling common "keywords" to companies such as search engines. One e-caller that's been bitten is 1-800-Flowers.com. When certain web surfers visit the site to browse for bouquets, a pop-up ad appears for \$10 off at chief rival fd.com. The same sort of thing happens at [americanairlines.com](http://americanairlines.com), where a Delta Airlines promotion is waiting in the wings. Ads like these find their way onto browser windows through "plug-ins" that come bundled with certain software downloads.

Keyword advertising consists mostly of selling trademark owners the rights to their own names - on a search engine, for example. But the reverse is true in many new application services such as Gator. And because the applications are downloaded with the consumer's consent, the companies say they are standing on firm legal ground, despite numerous complaints from marketing executives. After compiling the data it receives, Gator sells to other advertisers, who can then purchase the opportunity to display pop-up ads at certain moments, such as when specific words appear on the screen or specific words are typed into search engines.

### Gator/GAIN Modules

Gator (gator.dll and others) is the main software, which auto completes web forms (which is completely unnecessary for many users these days, since IE and Mozilla have had automatic form completion, password saving, etc. built in for some time).

OfferCompanion is the advertising spyware module. It is responsible for spying on your web browsing habits, downloading and displaying pop-up ads, and transmitting personal information to Gator.

Trickler (fsg.exe, fsg-ag.exe, fsg\* .exe) is an "install stub," a small program that is installed with the application you really wanted. (Gator almost always appears on your system due to installing other software and not the installer available from Gator's website.) When installed, Trickler inserts a Run key in your Registry so that it is silently and automatically loaded every time you start your computer. Trickler runs hidden and very slowly downloads the rest of Gator/OfferCompanion onto your system. It is suggested that this "trickling" activity is intended to slip under the user's radar, the steady, low usage of bandwidth going unnoticed. While often named fsg.exe, Trickler can go under other similar names, such as fsg-ag.exe (installed with AudioGalaxy) or another name containing "fsg" or "trickler".

### GAIN

(gmt.exe, CMESys.exe, GAIN\_NETWORK\*.EXE, other files) is short for Gator Advertising Information Network and is the newest incarnation of the Gator spyware we all know and love.

Each .exe file installs itself into a different directory. GAIN for example can be found in `C:\Program Files\Gator\` and the registry key `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows--\Current versions--\Run\GMT` is in `C:\Program Files\CommonFiles\GMT` and in the `C:\Windows\Start\Menu\Programs\Startup\`.  
CMIE can be found inside `C:\Program Files\Common Files\`.

### Removing GAIN/Gator

This is a somewhat long and annoying process, so let's get right to it. I must warn you it involves tweaking Windows's registry, so if you don't feel comfortable doing that, seek professional attention. There are several places you need to clean up, depending on how the software was installed. I will go over each step by step.

**Add/Remove Program Applier.** The best way is to begin by first uninstalling it through



the Add/Remove function in the Control Panel, since simply manually removing it may result in some of the components being left on your PC. To accomplish this, go to Start->Settings, open the Control Panel, start up Add/Remove applet, and hunt for either GM, Gain, GATOR, or any of the above listed modules.

**Windows Registry:** Click on START, go to RUN, and type "regedit". Click "OK" to start the registry editor. There are several keys you need to check here. First, using the directory tree, browse to the key: `HEX_LOCAL_MACHINE-->Software-->Microsoft-->Windows-->Current version-->Run`. If you got either CMEYSs and the GMT in the right pane, delete them both by using the right mouse key. Now you need to exit the registry editor and restart your computer.

Here are the other keys you should check:

- `HEX_LOCAL_MACHINE-->Software-->Microsoft-->Windows-->Current version-->Run`
- `HEX_LOCAL_MACHINE-->Software-->Microsoft-->Windows-->Current version-->RunOnce`
- `HEX_LOCAL_MACHINE-->Software-->Microsoft-->Windows-->Current version-->RunOnceEx`
- `HEX_LOCAL_MACHINE-->Software-->Microsoft-->Windows-->Current version-->RunServices`
- `HEX_LOCAL_MACHINE-->Software-->Microsoft-->Windows-->Current version-->RunServicesEx`
- `HEX_CLASSES_ROOT\CLSID\{21F9EBC0-0D41-11D5-89D5-00500413130C}`
- `HEX_LOCAL_MACHINE\SOFTWARE\GATOR\GATOR`

Using the directory tree, browse to those keys and delete them.

**Program Files directory folder:** Next, you will need to locate and remove both the CELL and GMT directory folders on your computer. They are both located in the Program Files directory. To get there, start from My Computer, go to Program Files, locate Common Files, and peek inside. If you see CELL and/or GMT, simply click on them with the right mouse button and choose Delete.

If Gator was installed by Precision Time & Date Manager, locate and delete the "WebPT" or "WebDM" inside the "Program Files" folder if it exists.

**Startup directory folder:** The next place to check will be your Startup folder. The Startup folder loads the software listed in there every time you start up or reboot the computer. To go there, start up from My Com-

puter, go to C:\, go inside Windows, and look for the Start Menu folder. See if any of the files listed above are in there. Remove them if you find any. This will have the added benefit of making your computer boot and run faster. Note that using the program associated with a particular ad-trojan may reinstall these references, and even the ad-trojan itself. PKZIP is notorious for this. (For this reason, it is important that you zap the associated adware program as well, or at least make sure nobody runs it.)

**MSCONFIG:** Under Windows 98 and higher, there is a program called MSCONFIG that allows you to view and enable/disable Startup applications. This can be used (usually) to turn off auto-loading spyware components. (To run MSCONFIG, if you have it, click on Start | Run, and type msconfig in the run box.) As you can see, msconfig is a System Configuration Utility and it's got several options you can modify. Let's now go over each one, briefly discussing what they are and what can be changed inside them. The Central option specifies what system files your PC reads and executes while booting up. This option is useful in case of an emergency during Safe Mode boot up. Normally, most autoexec.bat and config.sys files are empty today, but they used to play a big role in the olden DOS days (Windows 95 and Windows 98). If you know DOS (and DOS is still extremely useful in many ways, even if Microsoft makes it exceedingly difficult for you to even run DOS programs on NT based systems such as Windows 2000 and XP), you can peek inside those files and remove any lines you don't want or don't think you need. A good idea is instead of removing the lines to just place a REM in front of them.

**System.ini and Win.ini** are more Windows configuration files, telling it how to boot up. I suggest you don't mess with them unless you really know what you are doing.

**The Startup Option** is another more advanced way to tell Windows what software to run when it boots up. Personally, I like to keep mine as clean and tidy and program-free as possible. I have seen some people's computers that had at least 30 lines inside Startup, all from various software packages installed that did nothing for the user except take memory. I had to argue with a client several days ago, trying to convince him that in fact Microsoft's Office does not need to be inside Startup and that, yes, he still would have been able to use Office any time he wanted to. Talk about ig-

norance not being bliss!

How does yours look? Can you justify why all of the programs listed in there have to begin at boot up time? Do you know what each program is, and what its function is? Don't you think you should?

**Newton Knows Best**

This is another very annoying spyware or scumware or whatever you wanna call it that gets installed in a variety of ways, including with several file sharing programs. One of them is Grokster. I read about Grokster, one of the most infested of the P2P services, so I decided to see if it was really as bad as the writer claimed. I'm sorry to report it was worse.

When Grokster ran for the first time, a separate program popped up, asking me what my country and zip code was. It was called Newton Knows Best. Since I didn't remember allowing it to install, instead of just removing it I decided to observe what it was and what it would do. So far I am not very happy with it at all. It added an extra bar to my Internet Explorer that I had trouble removing. When I launched Netscape, Newton jumped up and started too. It even booted the self-updated Newton.exe. I was agghast. Yet another of the many shameless companies, who surreptitiously install software on my PC without asking me first, then begin to monitor my surfing habits.

I did a quick search on Newton Knows Best, but couldn't find much. Newton bills itself as a personal search companion. It claims it will help us get the most out of the Internet. Here is what they say at <http://www.newtonknows.com/netme/71/>: We designed NewtonKnows based on user functionality and benefit. As you surf the web, Newton sits discretely in the background, waiting to fetch relevant content for you. As soon as he digs some up, the Newton suggestion window slides up and presents his top finds. For example, "My Auction Items" fetches eBay auctions for your favorite items. Newton further enhances your browsing experience by delivering related content links directly into his toolbar. Newton quickly connects you to your favorite shopping, music, travel sites and more. With its built-in auto-update feature and our continuing commitment to quality, Newton will continue to evolve, and so too will your surfing prowess. Plus, with the ability to request your favorite new feature, Newton is destined to become your ultimate Internet search companion."

Newton made me see red in several ways, such as adding an extra search bar into Internet Explorer and not even asking me if I would allow it to do so.

**Removing Newton Knows Best**

This is somewhat difficult, since it places a key inside the registry and installs itself in several places. Run a search via Start->Find and uninstall. Don't just remove Newton. Hit the same places I outlined above in removing GAIN/Gator.

**SaveNow (When UShop)**

This gets installed by BearShare among others. Put quickly, it is an advertising toolbar that monitors what sites you visit and pops up sponsored "deals" when visiting those sites.

**Fighting Back**

There are several software packages that will help you to manually look for Gator and many other scumwares on your system. Ad-aware from Lavasoft (<http://www.lavasoft-usa.com/>) is a good one that has both a freeware and paid shareware version. It can help you remove remnants of programs installed surreptitiously on your machines.

Ad-aware is easy to use. Start it up and click on Scan Now. From there, you will be giving the following options: Perform smart system scan, Use custom scanning options, and Select drives/folder to scan.

Performing the smart system scan is good. Click on Next and let it run.

Once Ad-aware is done, you will be given a list of suspicious registry keys, registry values, and possible scumware exe files and folders. Click on Next.

You will be given the file name, what type it is (registry key or exe), what it is, where it is in your system, and comments that will even tell you what website was responsible for the scumware. If you hover over each with your mouse button, a yellow pop up screen will appear with more info. You have two options here: either quarantine the offending files or outright delete them by choosing Next.

As a precaution, I again must warn you some of your nice "free" programs won't be able to work if you kill their spywares, so before you push Next you must find what is needed by you and what you can live without. Some suggestions on how to find scumwares:

1. Begin using a process observer that will show all the software currently running on your system at all times. I can easily find and monitor any of these programs using the great and free Process Explorer from

```

http://www.systems.com/nw/2k/free
>vaxr/procex.p.shtml. Using it, I discovered
that GAIN/Gator-whatever you wanna call it
writes to the following files:
c:\windows\cookies\
c:\windows\history\history.ie51,
c:\windows\temporary internet
files\content.ie51
c:\WINDOWS\COOKIES\INDEX.DAT,
c:\WINDOWS\HISTORY\HISTORY.IE5\
INDEX.DAT
c:\WINDOWS\TEMPOR-1\CONTENT.IE5\
INDEX.DAT,
c:\WINDOWS\TEMPOR-1\CONTENT.IE5\,
c:\WINDOWS\Cookies\index.dat,
c:\WINDOWS\History_History.IE5_
index.dat
c:\WINDOWS\Temporary Internet
Files\Content.IE5_index.dat

```

Forget about ZoneAlarm. That's not good enough and it doesn't do much. I tested it several times, trying to figure out why so many people liked it. I think the main reason is because it is free.

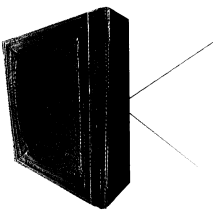
3. Run a weekly check on all the places I mentioned: Windows' StartUp folder, Registry's Run, msconfig. Keep them clean. There are so many scumswars confronting the average computer users today, it's easy to become overwhelmed! Worse, new ones are coming out daily! Keep up with them by reading sites such as <http://www.cexx.org>, or search for more info on your own.

4. Practice some self control and stop downloading and installing all the new hot P2P apps your buddies told you about.

This is just a small introduction into the world of scumswars. I would like to hear from other people about their own experiences with other scumswars so we can all learn.

# ClearChannel's

**DIRTY LITTLE SECRET**



**by Chris Johnson**

First off, a small introduction for those of you who don't know the evil that is ClearChannel. Clearchannel operates a bit over 1,200 stations as of the writing of this article. They also own 37 television stations and operate over 200 venues nationwide. They are in 248 of the top 250 radio markets, controlling 60 percent of all rock programming. They also do outdoor advertising and own the tours of musicians like Janet Jackson, Aerosmith, Pearl Jam, Madonna, and N'Sync.

Now we add a small division of ClearChannel based out of Cincinnati called Critical Mass Media into the mix. Critical Mass Media is the research arm of ClearChannel's radio business. CMM does audience research, music research, and also conducts telemarketing to businesses and res-

idences concerning contests or promotions the radio stations might be holding. Now here's the even more interesting part. CMM is exempt from the Do Not Call list. That's right! ClearChannel is using a loophole in the law to force its fecal matter into your home. Now, keep in mind, all dialing is done from either Norwood, Ohio or Fort Wright, Kentucky. If they say they are calling locally, they are full of crap. CMM hires only the best people for its delicate research. They recruit the vast majority of their individuals from temporary agencies. CMM holds three training classes a week at two days per class to train new agents if that gives you any idea on the turnover rate. They also pay these idiots \$8.50 an hour. If you're broke, it can be a lucrative opportunity for money.

Data from all calls is entered into a computer system referred to as CATI or the Com-

puter Aided Telephone Interviewer. It's powered by SCO OpenServer Unix in a dumb terminal style environment. CMC SURVENT is the main program used by the agent to conduct interviews. The agent has very limited access to the operating system. Most supervisory tasks including stopping and starting workstations is done by a section operator, referred to as CMM as a "captain" operator. Agents are monitored in several different ways including roaming or spot monitors done with cordless phones and by computer as well where a supervisor watches what they input into the system and what they are saying to the respondent. Any PBX phone in the call center can monitor an agent's station.

Now lets move on to how to identify a call from CMM. The easiest way is to watch for the number 513-858-2250 and the name HAMILTON, OH on Caller ID.

There are several different types of calls that CMM will place. First off let's discuss the "Audience" call. The rep will call your home and say "Hello, this is [insert name here] from [insert major city name here] Radio Research." This is what CMM does to probe for radio listening habits. Now keep in mind that during this call they will ask you a bunch of different questions such as name, race, and other additional questions that the station wants asked.

Then there is the "Screening" call. This is much like the audience call except if you pick the station they're screening for, they'll ask you an extra question: "Can you be reached at this number all year round?" and usually lasts around 30-45 seconds.

Let's say you got asked that question and you receive yet another call from them. However, this time they're asking for you personally and they identify themselves as "[insert city name here] Radio Ratings Center." If you agree to take the call, they will ask you some similar questions to the screener call above. If you pick the right station completing the ClearChannel trifecta, the rep will say "Now let me explain to you how this works" and proceed to read some responses and definitions. You'll get to listen to around 40 song books and be asked your opinion on each song. This is how stations figure out their playlist for the upcoming week. If a song (let's use Milkshake by Ke\$ha as an example) triggers 50 people to say that they have never liked this song, then the station will most likely pull it from airplay.

You're probably saying, "Why is that so horrible, Chris?" Well, the reason it is horrible is because of the method in which they contact you. On the day the project is due, they will not dial any number less than two times in one day and sometimes even more. I've seen one campaign where they redialed all the previously dialed numbers eight times in one day! They also will call your house every time they get a new project in from that radio station. Also, the other downside with this is if you say that you are not interested, then they simply note your file for a callback in a week. That's right, even if you tell them where to go, they will still keep calling! However, they'll just wait a week, maybe. The only easy way to get off their list is to tell them that if they call again that you are going to sue them.

Next we shall move on to the Perceptual. What this is is a full investigation of your radio listening habits. CMM will call and identify themselves as "[insert city name here] Radio Ratings Center." They first will ask a bunch of qualifying questions. If you qualify for this survey, be prepared to spend no less than 30 minutes on the phone with these folks. If you want to get out of it, however, just tell them if they call back you're going to sue the pants off of them. The agent is required to code your call so that the system automatically places you on their do not call list!

Last but not least, let's get to the Nest. Nest marketing is used by most ClearChannel stations. Nest takes a few different forms. I'm not going to describe them all here, but if you really want to know all the different forms this can take, go pay a visit to <http://www.criticalmassmedia.com>. Today we're going to cover the Nest "telemarketing" call. Now as far as I can tell, this is where CMM definitely abuses the loophole. Due to the fact that they are not selling anything, they are exempt from the law. Your phone will ring with the same number used by all of these other studies and a voice at the other end of the line will identify him/herself as "Chris Johnson," "Alex," "Chris," "Pat," or a few other cleverly disguised androgynous names. They will talk as if they are calling from the station itself and will want to add you to a contest or encourage you to listen at certain times. I will give you a hint. The

times they tell you to listen are key times for the Arbriton diary keepers. There is electronic monitoring equipment that can allow a station to make an educated guess as to how many listeners are actually listening to the station. The more listeners at those specific times, the more of a ratings share they can get, the more advertisers they can get, the more money they can make.

Let's talk about what happens if you demand a supervisor. One of the call center managers or supervisors will come to the agent's terminal and pick up the phone. They will give their name and ask how they can help. Most of the time these names are fake. There is one manager in the call center that generates a unique name for every supervisor

call. So it's a good sporting possibility that you don't really have that person's name. Also, if they give you the number to the "corporate office," 513-858-2250, it's only a VMMSI. There are no humans there. Ask if you should call 513-631-4266 instead. That's the real corporate office.

All of the above studies cost the stations thousands of dollars to complete. One estimate that I heard was that a Perceptual was around \$1500 per complete (they generally do no less than 300-400 completes on this type of project), a music call is around \$500 to \$700 per complete (generally around 100 people complete these), and an audience call is around \$250 to \$400 a complete (there are always around 420 completes).

# Impromptu Lock Picks

by L. Gallion

This article assumes you are familiar with lockpicking and lockpicking tools. If you are completely new to the subject, I suggest you Google for the *MIT Guide to Lockpicking* and read it before continuing.

To pick a lock, you need two things: a pick and a tension wrench. The pick is used to press on or rake across the pins inside a lock while the tension wrench applies a turning force to the lock's cylinder. The trouble is it isn't always practical (or even legal, depending on local ordinances) to carry professional lockpicking tools. Fortunately most homes and offices come stocked with all of the materials necessary to make your own basic tools.

For example, here are some items I rounded up in just a few minutes:

- 1) Fingernail clippers (the kind with a built-in nail file and a little hole at one end)
- 2) A couple of bobby pins
- 3) An old credit card (or any plastic card of similar thickness)
- 4) A couple of small paper clips
- 5) A large safety pin
- 6) A "Strong Fastener" (Acco #70022, used to

hold large printers together)

7) A good pair of steel scissors

8) A plastic cable tie (used to secure cables and wires together)

9) A round-head brass fastener

Using just these items and a little imagination, we can create several different lockpicking tools.

Let's get started with the most limited of our resources, the paper clips. Professional picks and wrenches are often made from hardened, flat spring steel, while paper clips are round, soft, and bendable. This means that paper clip picks are only useful against locks with weak pin springs and paper clip wrenches only work with easily turned cylinders.

To make a paper clip pick, straighten out one end of the paper clip (leave the other end curled up as a handle) and then bend the very end of the straight section into a small, sharp "half" sticking up (this is the classic half diameter pick shape). The easiest way to do this is to clamp (don't press too hard) about a quarter inch of the paper clip in the jaws of the fingernail clippers and use the clippers to bend the paper clip. Do this again about one

eighth of an inch in from the end to finish forming the half shape. The end of the paper clip should look roughly like this:

While too soft to work as an actual pin pick, a paper clip can be used to rake simple locks, like the disk tumblers you will find in most Steclease and Hon fitting cabinets, desks and overhead bins.

To make a paper clip tension wrench, unfold the paper clip as before (leaving one curled end as a handle) and then bend about a half inch of the straightened portion back onto itself. You will want to make the actual bend as small as possible, so use a hard object to press on the bend and "close" it as much as you can (the scissors handles work well here). Finally, bend the "handle" so the paper clip now has an "L" shape.

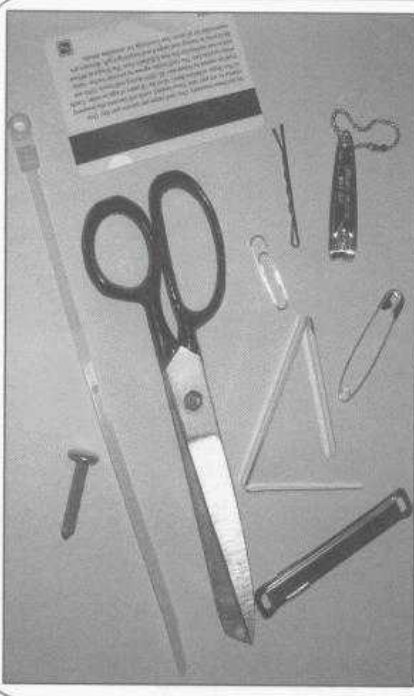
The bend at the end of the paper clip will usually fit into the bottom of the keyhole of most medium sized locks. However, a paper clip tension wrench is very weak and I have only used it successfully on smooth working deadbolts.

Now let's move on to a much better tool: the safety pin pick. Steven Hampton, author of *Secrets of Lockpicking*, says he got started using just a safety pin pick and a bent screwdriver as a tension wrench. Now you too can make just such a pick in seconds. First, carefully open up the safety pin and use the clipper's nail file to dull the point (so you won't

poke yourself). Next, insert the pin through the hole at the rear of the fingernail clippers. The pin should just barely be sticking out of the far side of the hole. Then, by rotating the entire clippers up or down, you can pinch and bend the portion of the pin sticking through the hole. Stop bending once the pin has a nice, gentle curve of about 45 degrees. Finally, open the safety pin up a little wider so it stays in a permanent "L" shape.

Being strong and made of flexible steel, your new-and-improved safety pin can be used as a hook pick on a variety of locks. I have successfully used it to pick five disk tumblers, four pin padlocks, and six pin deadbolts.

Next let's tackle another strong performer, the bobby pin. Bobby pins can be made into a good hook pick or a small tension wrench very quickly. First, remove the little plastic tips that come on most bobby pins and spread it apart so it forms an "L" shape. Next, insert the straight leg (not the way one) of the bobby pin through the hole in the fingernail clippers so that about a quarter inch sticks out on the other side. The tricky part of the bobby pin pick is that we want to put a bend along the thin edge (not the flat sides). To do this, tightly pinch the flat sides of the bobby pin about a half inch back from the fingernail clipper's hole. Then move the fingernail clipper up or down to carefully bend the bobby pin. If it starts to twist, stop and carefully



# Magstripe Interfacing - A Lost Art

by Acidus  
acidus@yak.net  
www.yak.net/acidus

Just like Sun Microsystems, people have been forecasting the death of magstripes for years. Yet they are still the most common form of physical authentication in the world. Their widespread deployment makes components for them cheap, and home brewed applications limitless. While there is a great wealth of knowledge on the Internet about magstripes, most of this is over six years old, mostly for very specific microcontrollers, or has out of date source code with no comments. Straight answers about how magstripes work and how to interface to a modern PC simply don't exist. I plan to correct that.

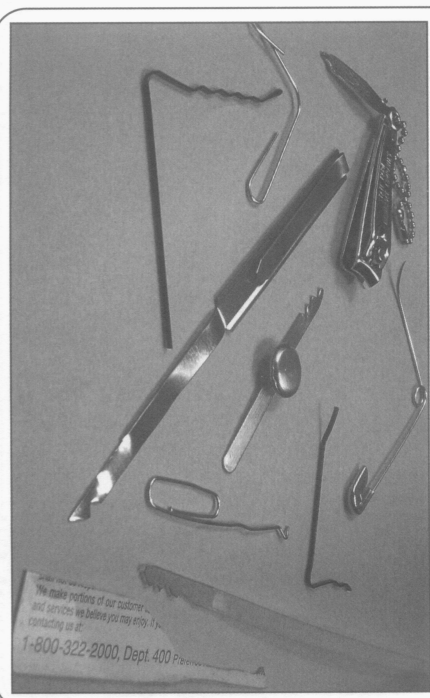
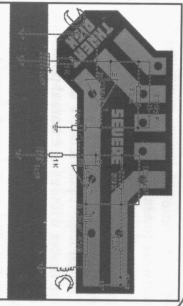
**Brief History**  
Count Zero wrote the definitive work on magstripes in November of 1992 for *Pirrack 37*, entitled "Card-O-Rang: Magnetic Stripe Technology and Beyond". While an excellent work, discussing the physical characteristics of magstripes as well as how the data is encoded on them, it contains no information about interfacing to magstripe readers. While several people have published works on readers and copiers, the definitive guide on interfacing readers to computers was written by Patrick Guellie in June of 1998 entitled "Interfacing a TTL Magcard Reader to the PC Game port". This work is extremely short, with no explanation of its Pascal source code.

It has been over six years since someone wrote something of substance about magstripe interfacing. The uncommented source code that you can find out there is so horribly dated that it will not run on any modern Windows OS (2K, XP). This article will explain in detail interfacing a magstripe to a computer, how to control it, and present easily ported source code that people can use.

**Magstripe Basics**  
See the *Pirrack* article for much more information about this subject. Magstripes consist of several magnetic particles held to a PVC card with a glue, and the orientation of these particles (and their magnetic fields) is how the data is stored. Magstripes can contain several tracks of information, each 110 inches wide. These tracks are defined by several standards; we are most interested in Track 2. This is the most widely used track, having been standardized by the American Bankers Association. This track contains up to 40 characters from a 16 character set.

So how is the magnetic representation understood by computers? Well, the reader contains a head which outputs an analog signal of the magnetic fluxes on the card. A specialized chip, called an F2F decoder, converts these signals into digital outputs. Interfacing directly to the analog signals would be insane, and F2F chips are critical for easy interfacing. Each F2F chip needs five volts (5V) and a ground (GND) as inputs, and for output has a Card Present (CP) line, as well as one to three pairs of Clock (CLK) and Data (DATA) lines, one pair for each track the reader supports. These F2F chips decode the magstripe data of each track as Bit Stream, using the CLK and DATA line. When the CLK line goes high, DATA line is the value of that bit (low=0, high=1). The CP line goes high when the reader detects that a card is being swiped through it. We will not use the CP line in our implementation.

**Our Approach**  
Using an F2F chip, we can read the bit stream of the data on the card. From the ABA standard, we know how those bits represent numbers and characters (shown in Figure 3). We simply need a way for a computer to read in the bit stream and write some software to convert it to the characters defined in the ABA standard. The good news is readers with built in F2F chips are easy to find and pretty cheap. They can be purchased from Digilkey, Jameco, etc. under the name TTL readers. You don't want to buy the expensive readers that connect directly to a serial or parallel



Page 14 2600 Magazine

straighten the twist out and then continue bending again. Stop bending the bobby pin when you have about a 45-degree angle. You have the proper shape when you lay your metal "L" down flat on a table and the end of one of the legs sticks up. The bobby pin tension wrench is a lot simpler: Just open up the bobby pin and spread it apart until it permanently forms an "L" shape. Although a great tension wrench, the width of the bobby pin is often too small to be used on a lot of locks. If the bobby pin wrench is too small, try using the nail file of your fingernail clippers. Just extend the nail file out to a 90-degree angle. The nail file tip will fit into the keyhole of some medium sized locks and the body of the clippers acts as the handle.

Credit card picks are easy to make but are only strong enough for one or two picking sessions. First, cut the credit card into about half inch strips. Next, use a straightened paper clip to measure the depth of the lock (push it in until you hit the back wall). Using this depth, trim down one end of the credit card strip so it is small enough to enter the top of the keyway. As you trim the end of the card down, shape the tip in either a half diameter or half round pick style (see the *MIT Guide* if you are not familiar with these shapes). Don't forget, credit card plastic is relatively soft, so try to use your fingers to support the thin shaft as you move it around within the lock.

Our final group of impromptu lock picking tools is a set of rakes. Rakes are pulled back and forth and up and down against the pins of a lock in the hopes of opening it. While raking won't have much of an effect against most high security locks, it works very well against desks, filing cabinets, and cheap padlocks.

Our rakes will be made out of the round head brass fastener, prong fastener, and the cable tie. Start by straightening out one of the thin metal legs on the brass and prong fasteners. Then use your scissors to carefully cut a series of "V" shaped notches or smooth "hills" at the end of each object (just on one side). Make certain the end is either pointed or sloped so that it can enter the keyway easily. You may also need to trim down the flat bottom portion of the rake to get it to fit into the lock.

Of these three rakes, I have gotten the best results with the cable tie. It's tough, flexible nylon construction allows it to move smoothly in and out of most locks. However, don't think that any of these makeshift tools are going to easily crack that high-security Medeco in your office. Advanced lockpicking takes a combination of skill, practice, luck, and the proper tools. But the next time you lock your boss's big presentation in a filing cabinet and lose the key, don't panic! Just use your lockpicking ability and a few office supplies.

We make portions of our customer... and services we believe you may enjoy... contacting us at: 1-800-322-2000, Dept. 400



port, as these readers will require special software to read from them.

We are going to adapt an approach shown in the Gentile article and interface through the game port. This has several advantages. The game port provides 5V and GND to run the reader without an external power supply. It has four easy to read inputs, game ports are usually free whereas serial and parallel ports are not, and even legacy free PCs without parallel ports, serial ports, or ISA slots still have game ports.

**Parts**

Getting a TTL reader is pretty easy. Digitey has a large section on them. Simply search for "mag card." Other online stores carry them as well. You want the simplest and cheapest one you can get. We are only interested in Track 2 readers. We don't care about cabling since we will make our own and we don't want motorized readers. We want the readers where you manually swipe the card (these are a lot cheaper). I am a big fan of the Omron V3A family of readers, specifically the V3A-4, since it offers exactly what we need. Expect to spend around \$15 to \$20.

In addition, you will need a DB15 male connector to plug into the game port. Make sure you don't buy a DB15 HD for VGA connections. Jameco part #15034 is what you want. You'll also need soldering tools, some wire, a hot glue gun, and some electrical tape. I used a few feet of speaker wire to connect the reader to the game port, so the reader could sit in front of the computer.

**How to Interface**

Make sure you can get the data sheet for your TTL reader and that it supports Track 2. Check the manufacturer's site. Using the pinout from the data sheet, solder wires to the 5V, GND, DATA, and CLK pins, making sure you are using the CLK/DATA pair for Track 2. If your reader supports multiple tracks, the contacts you have to solder to could be quite small; after soldering the wires, I covered the contacts on the reader with hot glue to make sure they wouldn't shift, break, or short each other out. Take your time and solder carefully.

Next, solder the ends of the 5V, GND, DATA, and CLK to the DB15 connector as shown in Figure 1.

A word of warning: not all the grounds on a game port will really be the grounds. Check us-

ing an LED to make sure the 5V and GND going to your reader are really active.

What we have done is soldered the reader

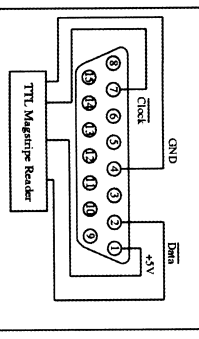
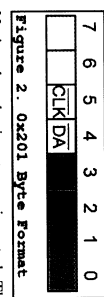


Figure 1. Wiring the Magstripe

outputs to the input pins on the game port that correspond to joystick buttons. We can now access the bit stream from the F2P chip as if we are checking the status of joystick buttons. We read from the game port by reading from I/O port 0x201. If we wired the reader to a game port as shown in Figure 1, when we read from I/O port 0x201, we will receive a byte whose format is described in Figure 2.



Notice that the inputs are inverted. This for each corresponding bit, 0 means a 1 from the card and a 1 means a 0 from the card. How do we read a byte from port 0x201? It varies from language to language, but is normally of the form "inp(byte = INP (address))." We then use "AND 16" to extract the DATA bit from the fifth bit of the read byte. This gives us the bit stream.

**Bit Stream Explained**

The bit stream of a Track 2 magstripe card looks like this:

```
[Leading zeros...] [start] [Data...] [end] [LRC] [trailing zeros...]
```

The data on the card is a 16 character set, represented by five bits, four for the character, one as odd parity. The character set for Track 2 is shown in Figure 3.

We are only interested in 0-9 and the start, stop, and field characters. They show us where in the bit stream we have valid data, and how that data is divided into fields. The number of leading zeros and trailing zeros

0-data bits-  
00 b1 b2 b3 b4 Char Purpose

0	0	0	0	1	0	Data
1	0	0	0	0	1	Start
0	1	0	0	0	2	Stop
0	1	0	0	1	3	Field separator
0	1	0	1	0	4	Field separator
0	1	0	1	1	5	Field separator
0	1	1	0	1	6	Field separator
0	1	1	0	0	7	Field separator
0	1	1	1	0	8	Field separator
0	1	1	1	1	9	Field separator
1	0	0	1	1	0	Control
1	0	0	1	0	1	Control
0	0	1	1	1	1	Control
0	1	1	1	0	1	Control
1	1	1	1	1	1	Control

Figure 3. Track 2 Set

vary, and are there to sync the clock inside the F2P chip. The trailing zeros are there so you can run your mag card backwards through a reader. Please note the F2P chip doesn't look for the start or stop characters, or anything like that. It simply reads the fluxes and outputs the CLK and DATA lines. Our program must scan the stream and find the start character. Once you find it, you know where the five bit boundaries are for each character and can read the data on the card. We are interested in all data from the start character to the stop character. The LRC is a checksum used to make sure the data on the card is correct. The source code doesn't check the LRC. Rarely is it necessary and for the most part any problems you have will be with the timing loop, as described in the next section.

**Problems**

Remember all those advantages for interfacing to a game port? There is one big downside. The game port doesn't generate an interrupt when a joystick is moved or a button is pressed. This means in our software we have to use lots of loops when reading the bit stream so we can trap the changes of the CLK line. To read a single data bit from the DATA line, we have to do the following:

- Step 1: Loop, checking for when the CLK goes high (and thus bit 7 goes low).
  - Step 2: Save the value of the DATA line (bit 5).
  - Step 3: Loop, waiting for the CLK to go low (and thus bit 5 to go high).
  - Step 4: If we still have more bits to read, go to Step 1.
- This is a time critical loop. The program has to catch each and every bit in real time since the bits are not saved or cached in any way.

If you have several programs running and your computer is off doing something else and misses a bit, the data will be wrong. How time critical it is can vary with language and hardware. On a Pentium 150, the PASM code from Luis Padilla Visdomine compiled and worked fine in DOS, but an implementation in Qbasic, even compiled, failed. The 3.4+ GHz machines of today should have no problem.

Lastly, a note on I/O port access. If you want to use my VB code and are using Win2K or XP, you will need to grab the Inpout32 from <sup>16</sup>. This is a DLL that allows you to directly access I/O ports under 2K and XP, which don't allow direct access like Win 9x and ME do.

**Source Code Explained**

VB is used because it's easy to understand and port, and I don't want the language to interfere with the explanation. The code is limited in that it will only deal with cards slid in the proper direction. It is heavily commented, so here is a quick overview. We read the DATA from the card just as described above, using a set of time critical loops. The array is sized to 240 since we will never have more than 240 bits on Track 2. We don't need to use the CP line because the CLK line will not go high until a card is in the track. After the first stage, our array contains entire bytes from 0x201 when we only care about the Data bit. The next stage uses "AND 16" to mask off the DATA from the fifth bit. The array now has only 1's and 0's, the raw bit stream. Next we scan the array looking for 11010. This marks the start of the data. Once found, we then read five bits at a time, looking for the end character 11111. When we find it, we read through the bit stream from the start character to the stop character at five bit intervals (since each character in the stream is five bits), and decode the characters using the chart in Figure 3. We appended these decoded characters to a string until we have read all the data between the start and stop of a Visa.

```
Account Number: 4313 0123 4567 8901
Expires: 5/06
Output:
^4313012345678901=05060102cccccccccccccccc?
The [0] after the expiration data is common to all Visa cards. See references below for many more examples of card formats.
```











# A Guide to Internet Piracy

by b-hstf  
charnass@hotmail.com

I've written this article after reading a few letters which show that some readers seem to know little about piracy on the Internet. I don't know everything about piracy on the net, but I would go so far as to say that I know a fair bit about it.

First off, piracy isn't just a few guys who work at cinemas and software stores taking the odd film or game home and sharing it on their home FTP servers or KazZaA.

Piracy on the Internet, or "the warez scene" (as those into it like to call it) is surprisingly organized. Pirated software/games/movies/anything are called "warez" and will referred to as that from now on.

## The Piracy "Food Chain"

**Top**  
*Warez/Release Groups* - People who release the warez to the warez community. Often linked with Site Traders.

*Site Traders* - People who trade the releases from the above groups on fast servers.

*FXP Boards* - Skripti Kiddies who scan/hack/fill vulnerable computers with warez.

*IRC Kiddies* - Users of IRC (Internet Relay Chat) who download from XDCC Bots or "Feservers."

*KazZa Kiddies* - Users of KazZaA and other p2p (peer to peer) programs.

## Bottom

We'll start at the bottom.

### KazZa Kiddies

At the bottom of the piracy food chain we have the KazZa Kiddies. There appear to be two groups of these KazZa Kiddies. First, the 13 year old kids with broadband downloading the odd mp3 here and there because they can't afford, outrageously overpriced, CDs from stores. Harmless kids, costing no one any real money, pursuing their musical interest. Also, these are the people being labeled "pirates," these are the ones "Killing the Music Industry." These are the ones who are being sued by the RIAA for thousands of dollars. *Sigh.*

Second are the older, p2p veterans who use other p2p networks (Gnutella, BitTorrent, EMule) and programs as well as KazZaA. In addition to using p2p for music, they may also download games, programs, movies, etc.

### IRC Kiddies

Not far up from the KazZa Kiddies we have the people who go to IRC for their warez fix. These folks can be more knowledgeable about computers and the Internet but tend to be just as irritating as the KazZa Kiddies. Warez Channels are often run by people who have access to a fair amount of pirated material (more about them later). There are generally two types of these Warez Channels:

*Feserve Channels* - These can often be run by the same KazZaA or IRC Kiddies; they don't really have a reason to run them; they just like to feel important. They mainly use the mIRC client's File Server function and some "133t skripti" to share their warez direct from their hard drives.

*XDCC Channels* - These are usually run by people into FXP Boards or Sitertrading. They have access to fast, new warez. They "employ" people to "hack" into computers with fast Internet connections and install XDCC Clients (usually troffer - [www.troffer.org](http://www.troffer.org)) which are used to share out pirated goods. From what I've seen, the people running these channels must primarily do it because they like to have power over a lot of people (being a chan op), but also they will often be given free shell accounts to run BNCs, Egegroups, etc. by shell companies in exchange for an advert in the topic of the channel!

IRC Kiddies can be found on EFnEt (irc.efnEt.net) or Rizon (irc.rizon.net). Other servers and channels can be found through [www.packetware.org](http://www.packetware.org).

### FXP Boards

FXP is the File eXchange Protocol. It isn't an actual protocol, just a method of transfer making use of a vulnerability in FTP. It allows the transfer of files between two FTP servers. Rather than client to server, the transfer becomes server to server. FXP usually allows

faster transfer speeds although it is generally not enabled on commercial servers as it is also a vulnerability known as the "FTP Bounce Attack."

*The Boards* - FXP Boards usually run Vbulletin (forum software [www.vbulletin.org](http://www.vbulletin.org)) and its members consist of Scammers, Hackers, and Fillers. There are also usually a few odd members such as Graphics People or Administrators but they don't do much.

*The Scanner* - The Scanner's job is to scan IP ranges where fast Internet connections are known to lie (usually university, etc.) for computers with remote-root vulnerabilities. We're talking brute forcing MS SQL and Netbios passwords, scanning for servers with the IIS Unicode bug (yes that three-year-old one). Oh yes, FXP Boards are where the lowest of the low Script Kiddies lurk. The Scanner will often use already "hacked" computers for his scanning (known as scanst0r's), using "remote scan" programs such as SQLHF, XScan, Fscan, and HScan along with a nice program to hide them (hiderun.exe) from the user of the computer. Once the Scanner has gotten his results, he'll run off to his FXP Board and post it. This is where the "Hacker" comes into play.

*The "Hacker"/Script Kiddie/slash Kiddie* - Now I think it's fairly obvious what the "Hackers" do. (They actually call themselves "hackers") Yes, they break into computers!

Their OS of choice (for breaking into) is usually Windows. There are many easy to exploit vulnerabilities and "nix scares these people. The Hacker's job is to run his application and "root" the scanned server. The program he uses (of course) depends upon the vulnerability the Scanner has scanned for. For example, if it's Netbios Password he will often either use psexec ([www.systemsadmins.com](http://www.systemsadmins.com)) or DameWare NT Utilities. There are various other vulnerabilities and programs used - too many to list here. Once he has "rooted" the computer (this usually means getting a remote shell with admin rights), he will use a technique known as "the ftp method" or "the echo method" (ftp -i IP get file.exe) to upload and install an FTPPD (this is almost always Sers-U) on his target. (In the case of the IRC Kiddies this would also be troffer). Once the FTPPD is installed and working he'll post the "admin" logins to the FXP server on his FXP Board. Depending on the speed of the compromised computer's (or "pubst0r"/"stro") Internet connection and the hard drive space, it will be "taken" either by a Filler or a Scammer.

*The Filler* - Now if the "pubst0r" is fast enough and has enough hard drive space, it's the Filler's job to get to work filling it with the latest warez. (The Filler usually has another source for his warez such as Site Trading). Once he's done EXPing his warez, the Filler goes back to the board and posts "leech logins" (read only logins) for one and all to use. What a great community!

FXP Boards are mostly full of Script Kiddies and people with too much time on their hands. They like to think the FBI are after them and get very paranoid, but in reality no one really gives a damn what they're up to except the unlucky sysops who get all their bandwidth eaten up because they forgot to patch a three-year-old vulnerability. The true "1000b" FXP Boards can be found on wondernet (irc.wondernet.net) so, if you like, go sign up on one and see what it's all about. Tip: Pretend to be female. This will almost guarantee you a place on a board. Say you can scan/hack dom, netbios, sql, apache, and have a 10mbit/10hour source.

### Site Trading

Next on the list, and pretty much at the top or near the top (as far as I've seen) are the Site Traders. These are generally just people with too much time on their hands who have possibly worked their way up through FXP Boards. Site Trading is basically the trading of pirated material between sites.

*The Sites* - These sites have very fast Internet connections (10mbit is considered the minimum, 100mbit good, and anything higher pretty damn good) and huge hard disk drives (200GB would probably be the minimum). These sites are often hosted at schools, universities, people's work, and in Sweden (10mbit lines are damn cheap in .se). These sites are referred to as being "legit." This means that the owner of the computer knows that they are there and being run. Fast connections mean a lot to some people. If you have access to a 100mbit line (and are willing to run a warez server there), there are people who would quite happily pay for and have a computer shipped to you just for hosting a site that they will make absolutely no profit from (you can meet them on EFnEt). Unfortunately, this is where credit card fraud can come into Site Trading. This is frowned upon by pretty much everyone (there is already enough paranoia and risk in Site Trading) but some people do use stolen credit card information to buy hard drives and such. To be fair, Site Traders aren't a bad bunch - the majority don't even believe in making any money out of it and insist that they are just do-

ing it for fun. Anyways, back to the sites, GLFTPD is considered to be the FTPD to use (in fact, a lot of Site Traders and warez groups will not join a site unless it is running GLFTPD). This also means that \*nix is the OS of choice (as there is no GLFTPD win port). As well as running an FTPD, the sites run an eegdrop bot with various scripts installed. The bot will make an announcement on an IRC channel whenever a directory is made or upload completed. It will also give race information.

**The People:** There are basically two ranks in site trading: "SiteOps" and "Racers."

SiteOps, as you will have guessed, are the administrators. There are usually between two and five SiteOps. One is often the supplier of the site, another the person who found the supplier and guided them through the installation of the FTPD. The others will be friends and people involved in the warez scene. One or more of the SiteOps will be the "nuker." It is his job to "nuker" any releases that are old or fake (more about releases shortly).

Racers are the folks who will "race" releases between sites. Usually they will have access to a number of sites and will EXP releases as soon as they're released. EXPing a release will gain credits. The ratio is usually 1:3, so EXPing 100MB will get them 300MB credits on the site, allowing them to EXP 300mb of data from that site, which will gain them 9000mb where they EXP that, etc., etc. "Racing" of releases occurs when two or more racers are uploading the same file. The race is to upload the most of the release at the fastest speed. Racing happens shortly after a release is... released.

#### Ware/Release Groups/"grps"

These are the ones basically supplying everyone with the warez. These are the ones the MIPA and RIAA don't seem to be too worried about, or at least aren't making a big public fuss about. However, these groups are known to the FBI and they know that the FBI and whatever other authorities are watching them and collecting evidence. They know that one day these authorities will strike as they have done in the past. A lot of these people are just hoping that they won't be caught when it happens. As a result of this, anyone "high up" is extremely paranoid. Most users will use multiple BNCs (Bouncers, an IRC proxy) before even going near an IRC network. A lot of large groups will own their own IRC Networks and SSL is used at every opportunity (FTP, IRC, etc.). It's hard to understand why these people actually do it when there is such a risk.

The main reasons are, in my opinion, boredom. At the end of the day, if you're sitting in front of your computer for most of your life you may as well be doing something other than flaming AOLers on IRC, and this sort of thing keeps you busy. Another reason is geekiness. Knowing that you were one of the first people on the Internet to see that film, or that it's because of you that thousands of people are now playing that leaked HalfLife 2 alpha and there are news articles everywhere about this "anonymous leaker" - it feels good, in a geeky kind of way.

A lot of these people (not all, not all) may have rather uneventful lives and to know that, although at school, college, or work they're considered a loser, they can go home at night and be looked upon as some kind of god within their group of online friends would feel good. I do not believe that profit is a factor. These groups insist that they don't do this sort of thing for money, and I believe them.

Here's a quote from a DEVIANCE .nfo file: *We do this just for FUN. We are against any profit or commercialisation of piracy. We do not spread any release, others do that. In fact we BUY all our own games with our own hard earned and worked for efforts. Which is from our own real life non-scene jobs. As we love game origins. Nothing beats a quality original. If you like this game, BUY it. We did!*

A quote from a Team Razor .nfo file: *SUPPORT THE COMPANIES THAT PRODUCE QUALITY SOFTWARE! IF YOU ENJOYED THIS PRODUCT, BUY IT! SOFTWARE AUTHORS DESERVE SUPPORT!*

#### Releases

A release is a piece of pirated material packaged and released by a warez group. The format of the release varies, but in the case of games or programs the release is usually in bin/cue, compressed with RAR, and split into 15,000,000 byte files. The naming of the release will usually be something along the lines of "NewGame3-RELEASEGROUP".

The types of releases vary. In games there are mainly either CD Images (bin/cue format) or Rips. Movies are either DVX/Vids (usually 600-800mb files) or SVCD/VCDs (two or three bin/cue files). There are many different types of movie releases. A great list of these can be found at [www.vcdquality.com](http://www.vcdquality.com). Releases will almost always be accompanied by a .nfo file. This will provide information about the release and the group.

#### Additional Info

The following information is not from first hand experience, like the past information has been. This has been obtained from text files.

told to me by people, and assumed. It will be mostly accurate, but there may well be errors. The main members of any release group are:

**The Supplier:** This is the guy working at the local cinema or games store, the guy with the digital camera happy to sneak it into the cinema, etc. Generally these people have to have access to new material, usually before anyone else gets to it. Often they will also have to have a fairly decent upload speed.

**The Cracker:** (only in games/apps groups) This will vary between groups. For example, a VCD/SVCD group would not require a cracker. But the cracker plays an important role. He will have to crack the game's protection that stops the game from being played without the official CD. This guy usually has a fair bit of programming experience and can be quite smart.

**Site Supplier:** Similar to Site Trading, however warez groups are often more picky about the sites they choose. The minimum speed is usually 100Mbit and often groups will only accept sites that are being supplied by the actual System Ops/Admins themselves.

**Courier:** This guy's role is basically Site Trading. He has to distribute the group's release to other sites.

Terms you may have heard and their meanings: **PRE/PRE'd:** When a release is released announcements will be made across many IRC channels called "PRE Chans." This is called the "PRE Time" and is the official time of release. **PRE Time** is used mainly in site trading. **0\*** This is a reference to how new the release is.

**Over:** This is a dream - n00b IRC Chans often use this term but they are lying.

**Onhour:** Means the release was PRE'd under an hour ago.

**Olday:** Means the release was PRE'd under an hour ago.

And so on...

**Nuked:** If a release is Nuked, the uploader of the release will lose credits on the site he is Nuked on. A release is Nuked when it is breaking site rules (like eight hours of PRE or ear-lying).

**Pubstrol/Sno:** This is a computer that has been compromised and has an FTPD running on it. It will be used to share warez, mainly to the FXD Community.

**Scan/Sno:** Similar to the above, but is used to scan for other vulnerable computers.

**Pub/Publishing:** Pubs are dead. These are from the old days when many university and business FTP servers had write access enabled

on anonymous accounts. So instead of breaking into a computer, the warez kiddies would just upload their warez and give the IP address to their friends. This was very popular but died out for obvious reasons.

**Tagging:** Once found a Pub would be "tagged" (a folder with the name "tagged by lamapubkiddie" or something similar would be made). The idea was that if a Pub was already "tagged" other Pubbers would leave it alone. This apparently worked for a while, with people respecting other people's tags and leaving the Pubs alone. But it certainly hasn't worked for a very long time.

**Dir Locking:** This was used in Publishing to stop people other than your warez group finding and downloading your warez (and slowing the server down). You would hide it, using directory names such as "com1" and "...". These directory names would also be hard to delete or even open, so it could take some time before the warez were found by the server admin.

**Raping:** The act of Raping an FTP server is when someone downloads pretty much everything they can from it at a very fast speed. It's frowned upon.

**Leeching:** Downloading a lot without uploading.

**PubStealing/Rehacking:** Back "in the day" this would have been referring to as uploading to an already tagged Pub. Now it means ripping someone else's Serv-U with yours. PubStealing is frowned upon and people will often be banned from EXP Boards if they are found to be doing it.

**Securing:** The act of Securing a pubstrol would involve deleting key files such as ftp.exe, ftp.exe, cmd.exe, etc. or changing the username/password. Securing methods depend upon the vulnerability.

Some warez related links: **www.njforce.nl** - a site that archives .nfos and releases. This site is frowned upon by people in "the scene."

**www.isomews.com** - a site seized by the federal government.

**www.vcdquality.com** - for movies specifically.

**www.fxp.nl** - fxp stuff.

**www.fxp.net** - rather large archive of fxp/script kiddie tutorials.

**www.packnews.org** - XDCC search engine.

**www.downhillbantic.org** - not related, but fuck the RIAA!

If I've mentioned a program and not given a link it's because it can be easily found through Google. That's all. I hope this has given someone a better view of piracy.

# Verbal Constricts

## Reference Material

**Dear 2600:**  
I am assuming you have seen this site before - but in case you haven't I thought you would like to add it to your bookmarks: <http://www.psyphone-directory.org/>. It seems funny that all the phones don't seem to accept any incoming calls anymore. I wish my phone didn't accept incoming calls either.

**Twigs**

*The online psyphone directory is one of our favorite sites on the net. It's well worth contributing to this valuable service. Unfortunately, so many phones can no longer be called due to the greed of the phone companies who believe a psyphone shouldn't be used unless it's constantly generating income for them. But it's still pretty cool to know where psyphones can be found and what location corresponds to which number. This info obviously already exists but for some reason the phone companies keep it secret.*

**Dear 2600:**

I don't know how known this is but I just found it and would like to share it with my fellow Hackers in School. If you go to <http://www.proxyfy.com> you can enter a url such as <http://www.2600.com> and go there anonymously, also bypassing the Cyber Patrol or whatever the school uses. There are more websites like proxyfy, such as <http://www.anonymizer.com>.

**Scott**

*It's pretty well known but it's always nice to learn of more. You can be sure that those people who don't want you going to our site will also be keeping track of these methods of bypassing their restrictions so they can find ways of blocking access to them as well. Meanwhile, here's another:*

**Dear 2600:**

This letter is regarding the letter by thesauravel in 21:1. I am a 12th grader at Gateway High School in Aurora, CO. My school also has similar software installed. This can be easily avoided by using an anonymous web service such as The Cloak (<http://www.the-cloak.com>). You can easily find such services for free just by searching Google for anonymous web browsing.

**X snipax**

## Gratitude

**Dear 2600:**

I've been published in peer-reviewed journals overseas. I've had editorials published in *The New York Times*. I've written instructional material that has gone out to every English-speaking country for computers at the top of the Fortune 500. Still, there is something especially satisfying about writing an article for a magazine of such infamy, especially considering that it has worldwide distribution.

**The Piano Guy**

*It's that special feeling that comes with knowing that you've just seduced your fate.*

**Dear 2600:**

My cat is obsessed with rubber bands, hair elastics, and generally anything circular that she can hook in her little mouth and run off with. Today she attempted to scoop up the red circle in the "no photos/no videos" picture on the cover of 20:4.

Keep up the good work. Even my cat is interested in 2600, it seems.

**SillyCardowner**

*Animals, toddlers, and aliens continue to make up some of our most loyal readers.*

**Dear 2600:**

I expected an April Fool's prank, somewhat in the same vein as last year's where the government "commanded" your site, but this year I was pleasantly surprised with the old-school games, such as Tennis and Pac-man, that you had on the site. Excellent job.

**mg488**

*If you're referring to our site somehow being patched into an April 2600 on April 1, let's just say the investigation is continuing.*

**Dear 2600:**

Having recently found myself working a retail job at a major computer retailer, I've noticed some promising trends. While I wouldn't say the average customer is any more technically inclined than you would probably expect, they seem to understand very well the rights that are being taken from them. For example, as soon as 321 Studios DVD X Copy was pulled from the shelf, I found myself constantly explaining what the DMCA is, how it is entirely too broad, and even some of the more technical aspects of how the program operated. While it's fairly likely my explanation of encryption, DECSS, rippers, and the likes were over at least a few heads, without exception people were genuinely concerned about their rights. Along with visiting the EFF's website, I recommended every person I talked to go out and pick up at least one copy of 2600. I've had more than a few people come back into the store thanking me for opening their eyes. So in turn, thanks for opening their eyes 2600.

**Redukit**

*This corresponds with many accounts we hear as well as those we see for ourselves. People just aren't as uninformed as those in power would like them to be. And even those who are uninformed often just haven't had the issues explained to them in an engaging way. When people realize the power they possess, they become a real threat to those who have been manipulating them. Fostering that realization is a worthy pursuit.*

**Dear 2600:**

I recently attended a high school in Greenville, South Carolina. Just today I went out to the local bookstore and picked up my first and only issue of 2600 - 20:4. I was reading through the letters and I think it's really awesome that you guys let everyone read people's opinions on education and technology. I have found myself getting

around the system once or twice in very small ways such as changing the security settings because all cookies were blocked so I couldn't login to my e-mail and things like that. I think we are very sheltered from the technological world when we are at school. It's the future. It's what we will live in. I know a few network admins and I have even met the district admin that I play little games with when he does such things as blocking my cookies. It's fun but then again I do realize it is his job to keep this from happening. As I was reading a letter from a South Carolina admin in 20:4 who was saying how he added 2600.com to the list, I decided to check it out for my district. No go. Like I said, in my opinion I think that they shelter us from learning about technology and its possibilities.

**Closer**

**Dear 2600:**

I wish to thank you for providing a magazine unlike all other magazines. I admire your bringing to the forefront many technological laws. I feel that it is uncommon for people to hear the companies and lawmakers behind bills and legal actions. I completely agree in your defending the creator of DECSS. I am glad that you used the magazine to inform people of bills such as the Patriot Act and Digital Millennium Copyright Act.

I feel that I can always trust 2600 to inform people of the truth about hackers. The overall feeling of sharing the knowledge is a true representation of the hacker community. I also feel that it is this sharing of knowledge that drives the technology community to correct the errors in their programming or equipment.

In conclusion, I thank you for everything that you have done and support your future efforts.

**Nick**

## Questions

**Dear 2600:**

Am planning to submit an article to 2600 later this month. I've noticed that there's a pretty high variance in the number of words/pages allotted to individual writers and so I was wondering if (assuming the content is interesting and not filler/fluff) there was any word limit, page limit, "target number" of words, or anything like that for missives intended for submission.

I imagine a 34-page tome would be disallowed as would a two-sentence "how to" on programming. "Hello World" in C#. But where (approximately) is the sweet spot?

Since I haven't written anything yet (sans a quick outline), your input will enable me to shoot for an article length that covers the topic effectively without making the Baby Jesus cry.

Thanks much for any advice you can offer!

**AB**

*The trick is to say what you have to say and keep it interesting throughout. All article submissions tend to get disqualified if any of us fall asleep while reading them. Length isn't really an issue if it's something we want to know more about. We prefer a long article that's thorough to a short one that's incomplete. And please don't send us material that you've already made available elsewhere.*

**Dear 2600:**

I am from Pakistan. I am really interested in this mag but I have one problem. If I send you a money order, what

confirmation will I have that you got the money order and that I will be getting the mag?

**Zero Cool**

*Different money orders have varying methods of finding out if they've been cashed and where. We suggest asking when you buy the money order. Assuming mail delivery is dependable in your area, you should have no problem receiving issues. Contact us if you do. You can also buy directly from our online store at <http://store.2600.com>.*

**Dear 2600:**

I recently took over a small office. The office uses a PBX phone system. Each month I check the phone bill carefully. I heard a rumor a few years ago that it was possible to hack a PBX and use it to call out for you. Is this true? How could I stop it?

**Kenneth**

*Not only is it true but it's very common. Checking the phone bill is a good first step. You should also check with the administrator to see if there are any ways to access the PBX remotely and if this feature can be turned off. If it's a necessary feature, check to make sure passwords are frequently changed and difficult to guess. Check your system's voice mail accounts to be sure that they're all valid and not being used as a camping ground for outsiders. If there are any restrictions you need on your system (such as restricting international calls or calls to premium services such as 900 numbers), be certain to implement them. Finally, make sure all of your lines bear the fingerprints of good security measures. All it takes is one mistake giving out a code or a dialup number and your job becomes orders of magnitude harder.*

**Dear 2600:**

I have the Secret Service following me everywhere I go. They have bugged everything I own. Ruined every relationship I have. They are messing with my bank account, etc. I have proof! I desperately need advice. I don't know why they are on me but I am way out of my league. And yet you don't show us the proof.

**Charles**

**Dear 2600:**

What the heck is this SSDI called SST-PR-1 that is all over the country? I don't buy the Sears truck explanation. Anyone able to elaborate?

**Ass Goblin**

*A little googling around indicates that this belongs to Sears (we believe SST stands for Sears Service Truck). There's a bit of controversy over whether Sears really has that many wiff-waddled trucks out there. Digging a little deeper turns up a press release showing that Sears worked with Intronix and Wireless Matrix to develop a custom laptop application for service techs which uses wifi to connect the laptop to the service truck and then either cell-modem or satellite data - depending on availability - to provide the backend to the Sears home systems. The \$85 million spent and the 10,000 units installed certainly seems to lend credence to the claims that it belongs to Sears, and this would also account for the frequency.*

*If you want something a little more intriguing to investigate, Wireless Matrix contacted in 2003 with the U.S. Department of Defense for "Remote Telecommunications Services providing service to a statewide division of the National Guard providing Homeland Security and emergency response services."*



**Dear 2600:** I am a privacy advocate and I was very happy to read the "Living Without an SSN" article in 20/4. I sent out a weekly newsletter to subscribers who are interested in fixing their bad credit and I would like to get permission to reprint this article in my next newsletter. I will include the author's name at the bottom and reference that it came from 2600.

**Rick**  
This is not a problem if you give credit to the author and the magazine. Please send us a copy as well.

**Dear 2600:** How am I supposed to disappear? I checked Yahoo addresses and backgrounds. Sir, I am everywhere. How can I function online and not be traced? How can I have DSL and not be traced? Is the only way not to use the satellite? And how do I clear my name? I am so tired of all the background and public records. Do I need to be reborn?

**Lynn**  
If you can't disappear you can at least muddy the water a bit by injecting all kinds of random bits of data into your profile. Use different addresses, different middle initials, add a letter or two to your name, write using creative handwriting style, etc. If you don't believe people need certain bits of info from you, then don't give it to them. By giving them something else, they're happy and you've added some cloudiness to your online identity. Just be careful that any bad data you give out won't keep you from using whatever service you're subscribing to.

**Meetings**

**Dear 2600:** First off, very good job on your magazine. I hope you can continue to be a great source of information as well as free speech for years to come (I am hoping that my kids will have something like your magazine to read in the far distant future). Second, I live in Miami, Florida. I was roaming the Internet late one night and I came across a web page for the 2600 meetings in my city. Much to my dismay I noticed that the page hadn't been updated since November of 2000. I am writing this in the hopes that whoever used to moderate these meetings reads this and may once again be interested in bringing them back to an operational status. I would try to do this myself but I am still very new to hacking and I would need some help.

**Isaiah**  
Our meetings don't require moderators - in fact, we prefer that there be no moderation at all. The idea of the meetings is to be open to everyone and we find that any hierarchy tends to intimidate newcomers and encourage cliques which is detrimental to the spirit of the meetings. Web pages were run by various attendees and if they're not updated they will simply fall off our list of pages or be replaced by better ones. Meetings however, will fall off our list if we don't receive updates from attendees on a regular basis or if they don't follow our guidelines. All of the info can be found at <http://www.2600.com/meetings>. So, despite your nervous, you have the ability to restart the meetings in your city. Good luck.

**Dear 2600:** I'm a longtime reader of the magazine and I also recently started to attend the local 2600 meeting. I found

myself in the situation where for the first time that I could think of I was able to sit down with like-minded people - people who I was able to find and who share the same thirst for information.

Like most things in life though I find that when you get into a good routine or find something good in life, something always comes along to put a damper on things and you back down to earth with a thud.

I found this happening to me in the past weeks and months. After attending a few of these meetings I found that I began to experience a few problems with my phone line.

In the beginning I put this down to prank calls, just some kids messing about I thought. But the strange occurrences kept happening. I decided to place a call to my phone operator to complain about the strange things that had been going on.

As usual the nice voice on the other end of the phone asked me for the usual information. Once I gave the info, I was thinking, "Yes, finally I'll get some answers." That was until she next spoke. I could tell by the sound of her voice that something in my the scared or spooked her or put her in a situation she didn't like. The stress in her voice was clear. She said, "I'm sorry sir but there appears to be some sort of problem with your account and you will have to speak with your supervisor."

Now at this point I was wondering what the hell was going on. A short time passed and again I got some stressed out sounding guy who I guess was the man in charge at the time. He said, "I'm sorry sir, we will try and solve the problem as soon as possible." I asked what the problem was, but he replied, "I'm sorry sir. I can't tell you that."

At this point I was convinced that something was up with my phone. I started to use my mobile a hell of a lot more when talking to friends.

For a week after the call to my phone company nothing else happened. But one week before the next 2600 meeting it all started again.

Strange noises, rings, then nothing on the other end with no Caller ID left, and strange clicking noises when I was using it, all just until a few weeks ago just before the last meeting. At around 7:30 or so I picked up the phone to call a friend when I got this started man on the line. He claimed to be a BT engineer. I asked him what he was doing on my phone line. He simply said, "I'm just testing the line. All is well and you can make calls." Now for a second I thought possibly it's all been in my head and this guy could just be faking the line. Then I sank in.

I'm not a BT customer, I'm not a BT engineer, I'm not a BT technician. For the next three weeks I watched and listened on every call I made to see if anything else would happen but it didn't. I still have little or no definite answers on this, simply a gut feeling and some strange circumstances that lead me to believe that for some reason my phone line was being monitored.

I know that I did nothing that would deserve this level of attention. So I guess I'm wondering why they're trying to do with the 2600 meeting that I was attending.

The end result of all of this was that I skipped a few meetings, although I now feel that was wrong. I mean why the hell should I miss out on talking to friends about stuff we're all interested in just because the government feels the need to monitor my calls. I know that in this day

and age things are bad and national security is a high priority. But just where does the line get drawn that separates matters of security from invasion of privacy?

**Tsun**  
Why do you assume there's a connection between this weird stuff and the meetings? You believe it has something to do with the meetings whether or not problems occur afterwards or if they're meetings with no problems occurring? The government spying on you. And even if it were somehow all related, this is no reason for you to sit on your hands. If someone harasses you for going to a meeting, we find the best solution is to let the world know with as many specifics as possible. But we're not convinced this is what's happening here. It could be anything from mischief to incompetence to something weird that we haven't thought of yet. Customer service reps have all kinds of strange protocols and problems expressing what's in front of them on a computer terminal. Keep trying and we're sure someone will eventually tell you what's being said about you on that screen. As for the BT engineer that they still maintain the actual phone lines that other companies use. Or maybe someone has been hooking their phone up to your line. Illegimately. Check your phone bill for any weird calls.

**Tricks**

**Dear 2600:** I want to congratulate you on keeping the mag alive after all these years as I have been a fan a long time. Please keep up the good work for many years to come. One observation: Go to any Wal-Mart and go to one of those windshield wipe selection terminals (looks like a small box with an LCD screen). Press and hold the center button while pressing one of the arrow keys. An option happens with each of the keys. Have fun exploring.

**Infrared**

**Dear 2600:** I'm sure that I'm not the first person to think of this but I thought it was worth bringing up. Some of the biggest credit card companies (MBNA Master Card for example) have these "temporary" credit card numbers that you can generate for use in e-commerce. The neat thing about MBNA's ShopSafe program in particular (and probably others) is that you can set your own credit limit! Let's say you want to try out an online service but don't want to get recharged if you forget to cancel. Just set the limit on that temporary card number to cover the cost of the trial only - this will block any attempts to charge you additional fees you didn't ask for because that account will be maxed out. This is especially helpful to avoid getting nailed by shady websites where the line, the print says that you have to cancel a certain number of days before the end of your trial to avoid getting charged additional fees.

**Brendan Boggsian**

You may have trouble with this system if you pay your credit card bill, thus clearing the way for more charges to come in. If however, the charges for the trial period is less than an amount they would charge you for afterwards, your plan should work.

**Complaints**

**Dear 2600:** If Apple would stop trying to make themselves a monopoly in their own market and use a standard PC architecture, they would get so much more business. I realize they do use some standard PC components in their computers, but the core components like the motherboard still have to come from Apple. Microsoft obviously didn't get where they are today by having good software. They got where they are thanks to everyone not having to buy PCs and their components from a single manufacturer. This created competition, which drove down PC prices and greatly increased their popularity.

Apple has some real breakthrough ideas, but the problem is that most people aren't going to buy a new, very overpriced computer just to use them. I remember back when PCs used to cost \$2600 without a monitor. But their popularity and competition has greatly reduced their prices. Yet Macs still cost close to the same, at least for a decent one. You can get a PC loaded with software, a monitor, and printer for the same price (if not less) than that of a Mac. If Apple were only smart enough to take advantage of the PC's popularity and price drop, I think they could greatly increase their market share. Unless Apple stops this anti-competitive crap, Linux will triumph over the Microsoft monopoly long before Apple even has a chance.

**Jeff**

**Dear 2600:** I have a serious complaint against you. The apartment next to mine has had hacker meetings for some time and things have gotten out of hand lately. I know it's 2600 because they're hanging a sign on the door.

I know they're hacking my cable modem because my connection dies every time they get together and I'll be offline all night. I get viruses too. They know my phone number and prank me with breathing and hang-ups until I disconnect my phone. These people even write stories about me and post them online. While they're doing all of this they blast their computer music at full volume and put the speakers up against my walls. The last straw was finding human feces in front of my door after their last meeting.

I bought a copy of your magazine to figure out their behavior but I'm still clueless. I thought you were about computers? I've lost my patience with this crap (literally) and I'd appreciate a response. I'd hate to have to involve the law.

**Vladimir**

We would love for you to involve the law. We would love to be held accountable for every group of people in the world who writes the number 2600 on their door. Because as we all know, that's all it takes to prove that this is a tightly knit conspiracy. In all seriousness, if you want to deal with this problem, it sounds like you already know who the perpetrators are. There must be some way you can deal with them locally. If you really read the magazine you would see that our meetings don't take place in apartments but rather in public places for all the world to see. So don't go assuming that anyone who writes down our name is somehow affiliated with us. Would you be complaining to the White House if they stuck an American flag on their door instead?

**Dear 2600:**  
I subscribed to 2600 after its release for the first quarter in 2004. I received the first quarter edition, which I had already bought. I feel cheated because I will only get three editions for the year and I paid for four. You guys are fair and I am exercising my freedom of speech. All I want is a quarterly for the first edition of 2005. Then when I get out of school I can become a lifetime member.

**No Mas**  
Simply contact our subscription department (subs@2600.com) and we can straighten this out. You don't have to promise future allegiance to us in order to get a fair deal. But it's important to designate what issue you want your subscription to start with when ordering to avoid such tragedies.

**Dear 2600:**  
In the last issue, I read a letter regarding website "protections" that disable right-click, view source, page printing, and site grabbing. I went to several manufacturers' websites and was pretty annoyed by some of the "protections" that the software afforded:  
**Print blocking:** What is wrong with printing? Can't I at least have some record of the page so I can get research or product info without having to go back to their web page every time?  
**Text selection blocking:** This is more of an annoyance to the lazy who want to copy and paste but what about product pages with long model numbers that I may want to search for in other places?  
**Offline viewing:** I usually print out a copy of a site or download it so I don't have to log onto the Internet to view it. (we have dial-up). I don't quite get this. People also use printing and offline viewing to compare products or to e-mail a site. This would prevent many uses of the site (it also prevents site snavgers).  
**Screenator stopper:** What is the point? Maybe to prevent people from grabbing pictures, but still, if someone was going to steal website design and layout (the site said this was a risk), then it would take a lot of work to transfer design from a picture to actual code.  
All of these examples show "non-hacker" uses of websites that these utilities stopped (although Mozilla was immune to certain features of one company's product). These utilities seem to limit the functionality of a page more than protect it.  
Oh, did I tell you that all of the manufacturers' sites that I visited were unprejudiced by their own product? What does that say?  
That was my few minutes of anger. I'm done now.  
**Joshua**

**Dear 2600:**  
As a subscriber and frequent advertiser in the classifieds section of 2600, I have often wondered why your subscription customer service is so outdated. I always have a hard time finding a phone number and a letter to 2600 sometimes more than once to get my address changed. The ads usually go in without a problem but I still have to mail those in too.  
I don't like feeding the postal service monster any more than I must and it seems like a lot of paper is wasted here that doesn't need to be. While environmentalism likely isn't this magazine's niche, I am sure that any

hacker worth his salt can find some level of agreement with any policy that cuts down on waste.  
A good man once told me never to complain unless I am prepared to propose a solution... so here goes. Why not have a form on your website where a subscriber can place their ad and update their subscription information? For security, make them upload a scan of their mailing label as an image (the JPEG or GIF only) for verification. On your side, your people would begin and see all of the tasks waiting to be done and route them to the proper departments or e-mail the person back and tell them when he set up to receive the ad and let them know their update has been processed or that their ad has been received.  
Leave the small mail process for those who need it or don't have a scanner or just like mail better, but an online option such as this would make your magazine much easier to deal with.

**Shortfuse**  
The idea is to verify your identity which the label solution is quite good at doing. While the post office will usually notify us of an address change if you move, they won't forward magazines so you may wind up losing an issue. Incidentally, this already can be done online (along with Marketplace ads) if you order from our online store. A copy of your original order e-mailed to our subscription department is usually enough to verify your identity, although you may get a call for verification. We will not store any subscriber information of any sort on our website so you can forget about that.

**Dear 2600:**  
I'm really sick of the file structure of the mirrors being changed every few weeks in Mandrake. This really limits the usefulness of CRPMM in a business environment.  
I support time Mandrake servers at customer locations and when it comes time to check for updates on them (remotely) - every damn time the stupid mirrors have shifted the directories around!  
The locations of old versions of the distro should never change. These Frenchies don't seem to understand this. I see a repeat of history developing here. Again the Germans (SuSe) will roll over the French (Mandrake), but this time there will be no one to save them.  
I am a club member - but don't think that counts for anything. Check the forums there sometime if you think you see complaints here. And why is it that there are sites that run message boards as a hobby that have better search functions than mandrakeclubs forums?  
What I want to know is: What changed after '92? That was the last good distro they put out. Did someone leave? Different boss? What?

I have put in a lot of time learning Mandrake and I am sad that it looks like I am going to have to switch distros because I need this shit to work.  
**Dr. Smack**  
We're so happy to be able to give people the opportunity to vent.

**More Info**  
There is a critical flaw in the "XP Compatibility Wizard" program, located in the Start - Programs - Accessories - XP Compatibility Wizard. This program allows

users to run older apps in a sort of emulation of older Windows OSES. I'm not sure myself how it works, but I assume that's the gist of it. In any case, you can either browse for the application or type in the full path of the program. This is where the flaw appears. Even if the policy file says your user cannot see the C: drive, you can still type in the full path of the app you want to execute. However if you run, say, the Command Prompt and that is blocked in the policy, you still cannot run it. One thing that I found I could run is the MMC, or Management Console. If the admin never blocked this app and never banned authoring mode, you have access to this. I don't pretend to have an MSCE or anything, so I might be wrong here. All I know is viewing the C: drive that should be hidden is a big problem.

**Winkman3**  
I have recently started purchasing your magazine at my local Borders Books and have greatly benefited from some of the information therein. I would like to call the attention of your readers to the book *Free Culture* by Lawrence Lessig. This is available as a free download at free-culture.org and, while I have not finished it yet, it is a great book offering some solid arguments against the RIAA's actions without condemning piracy. I have found this book absolutely fascinating and may buy the book myself just to support the author. It shows their hypocrisy and how the destruction of P2P is against the foundations of this nation. I think that everyone who is concerned with property rights, piracy, and the future of the Internet should download this and read it. Just don't blame me if you try to do it all on a CRT monitor!  
**Matthew "Blind-ear" Capone**

**Dear 2600:**  
This letter is a response to Anonymouse's letter in 20-4 suggesting that using sandpaper to rub off the reflective layer of a CD is a good way to destroy it. I'd like to clarify that such methods work for commercially distributed CDs (aka silverbacks) where the digital data is pressed into an aluminum layer and then glued onto a plastic carrier (the disc). Consumer recordable optical media (I'm assuming the kind you'd most be interested in destroying) instead records its data onto the dye injected into the carrier disc. The dye itself is what changes color in the presence of the recording laser, not the reflective material, indicating a pit.

By following Anonymouse's suggestion, you'd only make it marginally harder to recover the data, as the disc could be read via a laser with the pickup head mounted on the opposite side of the laser, detecting pits via transmission instead of reflection.  
Consequently, DeadPhanter's suggestion (also in 20-4) of using acid is probably a more secure way of randomizing the atoms used to record your data on a CD-R.  
**vectorsign**

**Dear 2600:**  
This is concerning Amtrak computer systems and their horrible performance. Amtrak set up their CTC system several years ago. Before the CTC system was in place all interlockings were manned by human beings. A few of the more vital interlockings still are (Zoo Interlocking for example). The humans were responsible for making sure trains were routed down the correct tracks and the correct signals were displayed. In case any problems arose there were switch/signals/rack maintainers on or about the interlocking station to quickly fix the problem. As the new computer system came into being, the manned interlocking became computer controlled by someone at a control board miles and miles away. I know from personal experience that the CTC system has gone down for several hours at a time at least three times in the last 12 to 16 months. This can affect the entire Northeast Corridor. If a switch problem is encountered maintainers now have to be called to the scene of the problem to assess the situation as there are no humans there to see what is going on. Meanwhile, repairing the system is not like at home. It can take 30 minutes at a minimum to do this. The system is a fail-safe one, always erring on the side of safety in case of a computer failure. They do not want trains running head-on into each other. The system is far from perfect and frustrating, but it is getting better. SEPTA (the railroad system in the Philadelphia area) has switched to a CTC system of its own. They experienced massive problems in the switch-over from human control to computers. The system they used is from a European firm which set up computer controlled systems for airports and never set up railroad systems before. I'd bet the system they had to call a tech in California. If this tech was out of town or on vacation, the problem would not get solved until the tech was available again. There were massive headaches for dispatchers, conductors, engineers, and the passengers trying to get where they were going. SEPTA has not had a major problem for another and things seem to be falling in line. I work on SEPTA's rail system and can tell you all of this from experience and a little inside information. About their ticket kiosks... no clue.  
**dasler73**

**Dear 2600:**  
The Prophet discussed unlocking DCT4 GSM phones. Thanks to a little time with this article and google, I'm happy to say I now have an unlocked DCT3 phone.  
In the article, he gave a short list of Network Provider Codes (also known as Mobile Country Code + Mobile Network Code). You can get the full list from <http://www.gsmworld.com/forums/gsm/for/index.shtml>, although they don't show which codes map to which area of a given country. While the article also listed three different T-Mobile codes, T-Mobile phones are only locked using 310-20 no matter what their physical network is, and they have also been migrating their physical network entirely to 310-26.  
Also, DCT3 phones are just as easy to unlock and use the same method as the DCT4 phones, just a different code calculation. I used <http://www.unlockme.com/> which has a great collection of information and a nice DCT3 and DCT4 calculator.  
**Unlocked**

**Dear 2600:**  
In issue 20-4, The Prophet's article "Unlocking GSM Handsets" was interesting enough to get me to finally unlock my Nokia 3650. In the process, I found a few omissions of details and some information that seems to be at least partially incorrect.  
While a definition was given for Network Provider Code, little was mentioned of it. The NPC is made up of

users to run older apps in a sort of emulation of older Windows OSES. I'm not sure myself how it works, but I assume that's the gist of it. In any case, you can either browse for the application or type in the full path of the program. This is where the flaw appears. Even if the policy file says your user cannot see the C: drive, you can still type in the full path of the app you want to execute. However if you run, say, the Command Prompt and that is blocked in the policy, you still cannot run it. One thing that I found I could run is the MMC, or Management Console. If the admin never blocked this app and never banned authoring mode, you have access to this. I don't pretend to have an MSCE or anything, so I might be wrong here. All I know is viewing the C: drive that should be hidden is a big problem.

**Winkman3**  
I have recently started purchasing your magazine at my local Borders Books and have greatly benefited from some of the information therein. I would like to call the attention of your readers to the book *Free Culture* by Lawrence Lessig. This is available as a free download at free-culture.org and, while I have not finished it yet, it is a great book offering some solid arguments against the RIAA's actions without condemning piracy. I have found this book absolutely fascinating and may buy the book myself just to support the author. It shows their hypocrisy and how the destruction of P2P is against the foundations of this nation. I think that everyone who is concerned with property rights, piracy, and the future of the Internet should download this and read it. Just don't blame me if you try to do it all on a CRT monitor!  
**Matthew "Blind-ear" Capone**

**Dear 2600:**  
This letter is a response to Anonymouse's letter in 20-4 suggesting that using sandpaper to rub off the reflective layer of a CD is a good way to destroy it. I'd like to clarify that such methods work for commercially distributed CDs (aka silverbacks) where the digital data is pressed into an aluminum layer and then glued onto a plastic carrier (the disc). Consumer recordable optical media (I'm assuming the kind you'd most be interested in destroying) instead records its data onto the dye injected into the carrier disc. The dye itself is what changes color in the presence of the recording laser, not the reflective material, indicating a pit.

By following Anonymouse's suggestion, you'd only make it marginally harder to recover the data, as the disc could be read via a laser with the pickup head mounted on the opposite side of the laser, detecting pits via transmission instead of reflection.  
Consequently, DeadPhanter's suggestion (also in 20-4) of using acid is probably a more secure way of randomizing the atoms used to record your data on a CD-R.  
**vectorsign**

**Dear 2600:**  
This is concerning Amtrak computer systems and their horrible performance. Amtrak set up their CTC system several years ago. Before the CTC system was in place all interlockings were manned by human beings. A few of the more vital interlockings still are (Zoo Interlocking for example). The humans were responsible for making sure trains were routed down the correct tracks and the correct signals were displayed. In case any problems arose there were switch/signals/rack maintainers on or about the interlocking station to quickly fix the problem. As the new computer system came into being, the manned interlocking became computer controlled by someone at a control board miles and miles away. I know from personal experience that the CTC system has gone down for several hours at a time at least three times in the last 12 to 16 months. This can affect the entire Northeast Corridor. If a switch problem is encountered maintainers now have to be called to the scene of the problem to assess the situation as there are no humans there to see what is going on. Meanwhile, repairing the system is not like at home. It can take 30 minutes at a minimum to do this. The system is a fail-safe one, always erring on the side of safety in case of a computer failure. They do not want trains running head-on into each other. The system is far from perfect and frustrating, but it is getting better. SEPTA (the railroad system in the Philadelphia area) has switched to a CTC system of its own. They experienced massive problems in the switch-over from human control to computers. The system they used is from a European firm which set up computer controlled systems for airports and never set up railroad systems before. I'd bet the system they had to call a tech in California. If this tech was out of town or on vacation, the problem would not get solved until the tech was available again. There were massive headaches for dispatchers, conductors, engineers, and the passengers trying to get where they were going. SEPTA has not had a major problem for another and things seem to be falling in line. I work on SEPTA's rail system and can tell you all of this from experience and a little inside information. About their ticket kiosks... no clue.  
**dasler73**

**Dear 2600:**  
The Prophet discussed unlocking DCT4 GSM phones. Thanks to a little time with this article and google, I'm happy to say I now have an unlocked DCT3 phone.  
In the article, he gave a short list of Network Provider Codes (also known as Mobile Country Code + Mobile Network Code). You can get the full list from <http://www.gsmworld.com/forums/gsm/for/index.shtml>, although they don't show which codes map to which area of a given country. While the article also listed three different T-Mobile codes, T-Mobile phones are only locked using 310-20 no matter what their physical network is, and they have also been migrating their physical network entirely to 310-26.  
Also, DCT3 phones are just as easy to unlock and use the same method as the DCT4 phones, just a different code calculation. I used <http://www.unlockme.com/> which has a great collection of information and a nice DCT3 and DCT4 calculator.  
**Unlocked**

**Dear 2600:**  
In issue 20-4, The Prophet's article "Unlocking GSM Handsets" was interesting enough to get me to finally unlock my Nokia 3650. In the process, I found a few omissions of details and some information that seems to be at least partially incorrect.  
While a definition was given for Network Provider Code, little was mentioned of it. The NPC is made up of

The MCC-MNCC, Mobile Country Code, and Mobile Network Code. The correct unlock codes will require that you have the correct MCC-MNCC for the provider that locked the phone. This is important to mention because the 3650, referred to in the article as being easy to unlock and also being my phone of choice, at least the one provided by ATT Wireless, has a few caveats. Failure to know and use this information could result in, as The Prophet said, five failed attempts and an "ultra-locked" phone.

The MCC-MNCC (a handy list is available at <http://www.yeldata.com/MCC-MNCC.htm>) is normally five digits. However some providers use "extended MNCC" making the MCC-MNCC eight digits in our particular example, the trouble comes in that some Nokia 3650s were shipped to the US market with Finland's MCC (244) rather than the US MCC (310). To determine which NPC to provide the DCT4 calculator for your 3650 locked to ATT Wireless (USA): If your IMEI (on my model at least, removing the battery alone (as suggested in the article) does not reveal the IMEI - the MMC card must also be removed - entering \*006# on the phone's keypad also works) begins with 351102500, use the provider code "MCC-MNCC 24407". For IMEI's beginning with 351102501, 351102502, or 351102503, use 31038 as the provider code.

After my second failed attempt at entering the "7# code, as suggested in the article, I googled a bit and learned that for the 3650, the first unlock code should be used. After entering the first code generated by [www.sirius.com](http://www.sirius.com)'s DCT4 calculator, my phone displayed "Restriction Off" and, indeed the restriction is off.

The drop down list in uniqueness (and other vendors) DCT4 calculator displaying "Type 1", "Type 2", "Grt-Im", etc. is a reference to other, earlier DCT3 flashing programs that also generate Nokia unlock codes. The difference is, I suppose, in the algorithm used to generate the codes. However since they all seem to pass the same checksum, I don't know if it matters which one is used. For what it's worth, I used "version 2" codes, since the information available online indicates that these are known to work across all Nokia phones.

I hope this was useful. What would be nice would be for someone to write an article about obtaining domestic pre-paid SIM cards in the US. Pre-paid SIMs can be purchased for international minutes and there is a rumor that you can sometimes talk a reseller at a kiosk or storefront into separating a phone and a SIM from certain carriers' bundles but I have yet to find any definitive information regarding who or how to ask, or about social engineering that may be helpful in talking a reluctant sales rep into selling something that most carriers really do offer, but not promote. I really don't want an extra phone just to obtain a SIM in the States.

ScottVR

**Dear 2600:**  
In regards to an article published in 20-4 about Verizon's Call Intercept and its PIN being the last four digits of the home phone number, the same holds true for Verizon Wireless cell phones (and just about every other carrier out there). The security settings in the menu on the cell phone prompt you for an unlock code which is the last four digits of the cell phone number. I would advise your readers to change this number just in case your cell

phone falls into the wrong hands of someone who knows what they are doing.

Also, if anyone needs a six digit security number for a cell phone, I know two. Motorola is 00000 and Nokia is 123456. These codes should work for all models.

I hope this info helps someone out there.

SIRKRX

**Satellite Radio**

**Dear 2600:**  
This is a response to your response to maintainingun on page 36 of 20-4. I've been recording XM broadcasts for my own personal use through a customized (TOSLINK added) Delphi receiver for a while now. It's great. The only problem I have with it is that there is no way to read the track information from the broadcast and fill in ID3 for the recordings automatically. As for the RIAA this is one arena that they can't touch. It's already been ruled that time-shifting of TV and movies is lawful fair use, as is digital space-shifting of music. Not even they are stupid enough to challenge the digital time-shifting of music. I hope that they are concerned about this, because there's nothing they can do about it, and I'd hate to think I'm not doing anything to piss them off. Great msg, keep up the good work!

M@

**Dear 2600:**  
In a recent issue of *Nuts and Volts*, (October 2003) an article was published on SIRIUS Satellite Radio. Some of the specs published are very similar to what XM Radio uses, which would help one understand and see the potential weaknesses.

According to the article, SIRIUS uses QPSK (Quadrature Phase Shift Keying) for its modulation scheme. There is a QPSK (four level) decoder out that is used for Flex decoding of pager datastreams. The schematics for this are available on the web and are less than \$10 in Radio Shack parts to build. The PD102 and similar decoders will not work as they are simply level converters for two level (binary) decoding.

The frequency for SIRIUS is 2.32 GHz and the signal bandwidth is 12.5 MHz wide for the whole system. This includes both satellites and a terrestrial repeater for the hard to reach spots. According to the article, each of these gets a 3MHz of bandwidth or so.

The raw transmitting rate by transmitter or satellites is 7.5 mbps which includes the music, correction, and overhead as mentioned in the article on XM in 2000. The claimed audio data rate in the *Nuts and Volts* article is 4.4 mbps divided into 100 channels. This gives each stream about 44 Kbps, give or take depending on the quality of the encode. 44 Kbps is easily decodable on the XS-232 serial port so the Flex decoder mentioned above would be a good start. There was a sound card based decoder out but I never had any success with it and favored the serial port for decode.

You will need a receiver. My favored Icom R-7000 receiver will not go past 2.0 GHz without an external converter, although the ICOM R3 and the Winradios will. Myself, I'd find an in-chip XM or SIRIUS receiver and pull it apart and probe it with an oscilloscope and find an acceptable point to tap the datastream. Alternatively there are receiver kits in the ham radio market and plenty

of plans that could be modified from the 2.4 GHz ham frequencies down to 2.32 GHz if you have a bit of electronics knowledge.

However, a QPSK decoder may not work if they use TDM (Time Division Multiplexing). Being that each audio encode would have a time slice in the bitstream, at a minimal 16K encode for example per channel would give you 1.6 megabit worth of stream, not including overhead. This would be over the limit of a serial port by quite a bit. The QPSK decoder would need additional modification to sync up with the bitstream and just pull the bits corresponding to the channel you wish to decode.

If they use FDM (Frequency Division Multiplexing), then the QPSK decoder would work if your receiver can narrow in on the frequency slice of the data you want. Most likely pretty easy if you pull the data off the receiver chip on the satellite radio receiver. If you're using some other receiver for decode, or an external receiver connected to the IF (Intermediate Frequency) stage of the satellite receiver, then you will need to have the proper bandwidth set so you don't get trash data from data off to either side of what you're trying to decode.

I have not seen any block diagrams, schematics, or any hard data as to what is going on inside these commercial satellite radio receivers. You may be able to forego the QPSK decoder and find a pin on a chip spitting out serial data. It could be parallel data. I just don't know. It could be in the clear or encrypted. But unless someone probes and tinkers, you'll never know what can be done, what flaws, or even what other kinds of data may also be transmitted across the bird. The world of RF (Radio Frequency) is a jungle of all sorts of media such as voice, video, and data. 802.11x and Bluetooth are not the only RF medium that has Internet and other data. You'll find IP and networking data or Motorola's Astro Radio Systems that are being implemented in the newer public safety and government systems. There are two way Internet and data being transferred via DSL, via satellite, OpenSky, etc. You just gotta know where to look in the RF spectrum, or accidentally stumble across it.

For you coders, a good foundation in CRC (Cyclic Redundancy Checks), Reed-Solomon, and convolutional coding is definitely a plus. Some knowledge in encryption/decryption is also a plus. Yes, some of the satellites use heavy encryption. So did DVDs, broken by seven lines of code: DECSS.

Once someone figures it out as far as XM and SIRIUS, there is some fun to be had with recording software. Being that the artists name, song name, album name, and record label is encoded in the bitstream, you could easily record things by key word search. Or say you were trying to build an MP3 collection. The recording/decoding software could write the song name as the file name and the artist name would be the directory name.

Of course all of this does not just apply to audio stuff. There are all kinds of similar things to be done with satellite TV. Technotrend has come out (as have others) with the DVB-S 1.6 PCI satellite card. Linux drivers are available on [linuxdvb.tv](http://linuxdvb.tv). Some of the personal video recorders (PVR) such as the Newswave Plus, DCSStation Relook 3000, and others run Linux. A lot of the PVR/satellite receivers have RS-232 and USB ports to probe and exploit. [www.telesatellite.com](http://www.telesatellite.com) is an excellent site to check out for various PVR and satellite TV boxes. Granted, a lot of

the stuff on the site is for overseas satellite TV transmissions but some are receivable here in the U.S. DirecTV and Dish Network seem to be the trend but the KU, C, and S band satellites are cranking out 15,000 plus channels across all the birds. That is what the consumer is supposed to see. Minimal easy to do modifications can provide one with phone calls, data, and studio back channels to monitor. Like I said earlier, it's a jungle in the RF world.

Stormbringer  
I would enjoy exchanging letters and discussing theories or whatever.

W.K. Smith, 44684-083  
FCT Cumberland, Unit A-1  
PO Box 1000  
Cumberland, MD 21501-1000

**Call For Info**

**Dear 2600:**  
First off, you guys do an awesome job keeping the flow of information going strong and I gotta give my respect to that first and foremost.

My letter is sort of an open call. Recently in my area SureWest has started offering Broadband over IP offering television and Internet over IP on Ethernet. I finally saw the system which basically has a router on the outside of the house and then runs cat 5 through the house. Computers connect directly to the wall without any need for a modem, televisions use a set top decoder from Amnmo Technologies and use a company called Indeo Access for their "conditional access system." Each set top has a card that slides in telling the box what channels are allowed.

Does anyone know how this technology works? I assume that each wall plug has all information for both television and Internet and that the computer can only access the computer data since it has no idea what the signal for the TV means. But would it then be possible to run something like a hub or router off the wall and have it work for television and Internet? Could you somehow hack the card used in the Amnmo box like people do with their satellite service? I haven't found any information on either subject and thought the folks over at 2600 might see this as a new challenge.

Miles

*Our pages are open for some in depth discussion on this with as many specifics as possible.*

**Dear 2600:**  
I have acquired (through legal means) what appears to be some sort of credit card swapper/reader. The only name on it is Micros Model #400412 User worststation03. It has a large touchpad and when I plug it in it gives me the options to adjust the contrast level. It has two com ports in the back as well as an AT keyboard plug. A PC port (cat 5), two cash drawer ports that look identical to the keyboard port, a printer port, a larger than usual video port (labeled Cust. Display), and another port (labeled EXT port) which also resembles a cat 5 port. I am looking for any information anyone may have on using this device and exactly what I can modify it into.

mustangdriver504

More From The Military

Dear 2600:

In response to the letter from Neo in 20-4, tell your friend not to worry. I am in the military and an avid reader of 2600. One day at work I was reading the latest issue. Being in a career field where you deal with sensitive information on a daily basis, someone overreacted and informed my shop supervisor that I was reading potentially compromising pamphlets or some other crap like that. The next day I went into the flight commander's office to retrieve it back and he told me about what happened. Then he informed me that it is our duty to uphold and defend the Constitution of the United States and part of that is "the right to free speech" and that my reading this would fall under that. So Neo, to make a long answer short, if your "friend" gets in trouble, just tell her to read the Constitution next time someone tells her that she can't read 2600.

Caps Lock

As with anywhere else, you may be obstructed by minors and chads. But it's nice to hear of situations where rational thought and respect for freedom win.

Positive Stuff

Dear 2600:

Surfing around in an attempt to find a "bristle-block" explanation for a friend on encryption, I came across this on "How Stuff Works." It's good to see that some can get the idea and not spread ignorance. Here is the full text: "Somewhere between the locksmith and the burglar is the recreational lock-picker, sometimes called a hacker. Like expert computer hackers, their code is to pick locks for the fun of it."

scottr

Dear 2600:

Finally, a definitive answer on whether or not 2600 represents good hackers or not. The gentlemanator says 2600.com is 64 percent good: http://homestead.org/~gentlemanator/

Steaming Martyr

What a relief! Especially since the WPA was rated as 73 percent evil.

Submissions

Dear 2600:

I wanted to know if you've ever published an article on how to get all the screensavers, mungers, games, etc. on your Sprint phone for free. I have about two and a half years of 2600 and didn't find anything like this. If you haven't, please let me know and I will submit something I wrote about this for review.

mike

This sounds like something we'd be interested in. If your article is written especially for us and not directed up on a web page or published elsewhere then please send it on in. Online, you can email articles (ASCII format please) to articles@2600.com. In the real world, you can send mail to 2600 Editorial Department, PO Box 99, Middle Island, NY 11951, USA.

mlmmaster

Dear 2600:

Can you guarantee the anonymity of submitters of articles? I have an article that may make a large corporation very angry.

Anon Ymous

Your publication keeps a significant percentage of the corporate world in a perpetual state of angst so your article would be right at home here. If you take sufficient precautions, such as not using a phone that can be traced back to you, being specific as to which name we should use, and not having anything that could identify you in the actual text of the article, you should be OK. Also, be sure not to e-mail us from an account others might monitor, especially one from the large corporation itself. We can't discuss the possibility that e-mail traffic could be monitored somewhere along the line so in real sensitive situations, drop it in the U.S. mail with no return address. We're glowed.

Dear 2600:

Are the images that appear along with the articles supplied by the authors or do you guys add those in yourself? Or is it a little of both?

drifter

Yes.

Warnings

Dear 2600:

Rumor has it that there are two very powerful, radical fundamentalist cells operating in the United States. These two very large cells, comprising millions of citizens, each claim to trace their group conception to a little-known band of terrorists who once plotted and successfully carried out radical, military-style attacks on centers of authority right here in North America.

As November draws near, it is suspected that one of these two groups might try something dirty, underhanded, or even dangerous in order to affect the outcome of the presidential election.

Americans are urged to keep their ears open and to report any suspicious activity occurring near important political centers such as voting booths, press releases, and fund-raisers.

If you, or anyone you are spying on, receive any information about the activities of members of "The Democratic Party" or "The Grand Old Party," please notify national security authorities immediately.

eyenot

This is going to be our interesting year.

Dear 2600:

VerSign has a product called NetDiscovery that looks to basically be outsourced CALEA (Communications Assistance for Law Enforcement Act - http://www.fcc.gov/calea) processing. They just announced a deal with Cox to provide this for VoIP on Cox's cable service. This is one of the first in what will probably be a series of "preemptive" compliance with CALEA, seeing as the FCC is currently debating whether or not CALEA applies to VoIP. Anyway, VerSign has a "user's guide" for NetDiscovery available on their site, but it's password-protected (i.e. "customers" only). It seems like it might make interesting reading. http://www.verisign.com/cds/mkt

Discovery/secure/ctd/DiscoveryGuide.pdf

Dear 2600:

Just got a link in my e-mail that pointed to a phony web page on a Russian server which immediately opened a real ChatBank web page in a small phony page skinned for a bank bank number, PIN, and account number. The real web page from a FortLindner mail server, which alone should be suspicious. The Russian web server they parked on is a free web-based e-mail service. My guess is that the server had been hacked to place the fake page or some person working on the premises participated in the scam. I alerted ChatBank through their web-based message submission form. Thought you might find that interesting.

Dear 2600:

In the past few months, ever since this "wireless boom," I have become more and more concerned about the state of the 802.11 ad hoc networking. I say this because I don't need to go war driving. You heard me, all the APs I find are by accident. Ever since I started messing around with 802.11b, I have come across many unsecured networks that wanted to let me in. The secured ones were a joke. I know the default IP's of the AP's and a windows box will tell you the default IP's, and the default password is not hard to find (you printed it in 20-4!).

People don't realize how much of this is already out there. Even I didn't until recently. All the cool new laptops have it, PDAs, elevators, refrigerators, and these "hot spots" that they tell us about are popping up faster than rabbits with Mountain Dew.

Back when you needed a physical connection to get into a router it was somewhat easier for the manufacturers to make their devices secure by obscurity, but now that people can be outside and just get it, it's pointless. The manufacturers of these things don't care, the users don't care, the only people who do care are the ones who want to exploit it. With my AP I have taken every action I can think of to secure it (short of grounded aluminum foil on the walls and ceiling), but does it matter? There is so much unprejudiced wireless out there for people to get into that I don't think it does.

I think we are going to be in for a wake-up call really soon when the powers that be realize how rampant this has become. Don't be surprised if some new regulations come out, making sure you keep your networks safe from the evidences of the net.

I hope anyone who has this technology will secure it or get busted for downloading kiddie porn that they didn't even know the script kiddie perv next door was using.

wrathtype

Do you really believe new laws and regulations are the way to address this? What's happening now with wireless is the equivalent of wide open PBX's of days past where people would be able to make free phone calls courtesy of numerous corporations. Even now there aren't huge phone bills being generated. If companies today don't care enough to secure their wireless connections, they'll run the risk of having internal data compromised. That's what this should be held accountable for, not the specifics of what is sold or transferred by manufacturers. Apart from some companies not being vigilant with their own security, we see the prevalence of free

wireless connectivity (much of it intentional) as a very positive development.

Dear 2600:

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety. Ben Franklin

Will you please stop telling us this every damn day?!

Dear 2600:

A friend of mine has been having a problem with SBC Long distance and their Juno Internet service. There appears to be some kind of malware that consistently sets the victim's Juno access number to a number in Calgary, Canada. The victim lives in Missouri, so they then make a long distance call whenever they use Juno. The "gui bono" is SBC, who gets to collect a long distance charge. I am hoping you will print this so that others who know people in this situation will encourage their victim friends to report these incidents to the FBI so some action may be taken against the perpetrators of this scam. Hopefully Juno will take some steps to make changing the access number their software uses harder to change - perhaps a checksum or some other preventive measure could be put into place. Ideally SBC will refund all the long distance charges attributable to the malware.

KT

A fresh install of software sounds like it's in order here. It's also possible to monitor whatever numbers are being dialed on the screen as they're being dialed. You may also be able to install a block on this number through your local phone company.

Stupid Stuff

Dear 2600:

At the three different newsstands where I get my copy of 2600, there is always some sort of sticker on the logo and the word "hacker." Most of the time there is more than one. The stickers are the same stickers used for the price but there is no price on it so it is obviously with the intent of hiding the "hacker" word and the "2600." Being of positive mind, I entertained the idea that it was to protect the customers. Not being stupid I know better.

Fairy Book

Try to find out if these three newsstands are owned by the same people. If so, it's just one dandruffhead who thinks s/he's keeping something "offensive" from the eyes of customers. Why they bother to try and sell our magazine with that attitude is beyond us. If they're not owned by the same people this could be happening at some other level which we would love to find out more about. And there's always the possibility that this is just random stupidity on the part of the person doing this, not realizing that they're covering both the name and description of the magazine. Not likely, but stupidity is always possible.

Dear 2600:

I thought you would find it interesting that on the NOCTI (nocti.org) Computer Technology test (besides being completely obsolete, containing questions that applied to late 80s DOS-based PCs), one of the questions was written exactly as follows: A computer hacker is any person who

Continued on page 48



# CONSUMER SPOOKWARE VS. YOUR CASTLE

by wildbeard dreamer  
(a.k.a. dark spectrum)

It's been a long day. You slaved for hours under the baleful glare of your employer's closed-circuit spycams. You ran errands on city streets, in a mall, and at an ATM - more spycams. Then you visited with some friends at a wild party. Everyone there seemed to be flashing camera phones. Who knows how many wireless cameras and microphones were planted or where. But now you're home and you can finally feel that you have some privacy and security. After all, you've got bars on your windows, high-quality door locks, and an alarm system. You're surrounded by a protective shield of drywall, structural timber, and bricks. You swept the house for wireless surprise packages just last week. Still, you can't help asking yourself: are there any chinks in your armor?

You bet there are. Not just chinks, but big, gaping holes: clothes dryer exhaust vents and air exchanger vents. Stove vents, chimneys, and sump drains. Bathroom fan ducts, soil stacks, and sewer lines. Most of them are big enough to drive a truck through (a stripped-down 1.24 scale RC truck that is). You might be asking yourself "Ducks? Vents? Has this guy been playing too much Half-Life?" but in fact each of those external interfaces constitutes a vulnerability. Some of them are already borderline exploitable with consumer spookware available at the nearest big-box store. I'll give a few examples later on, but first a short history lesson.

This article describes the next phase in the ongoing erosion of your physical privacy. Phase One started over a decade ago with "Big Brother" spycams watching out for you. They were installed in public places, places of work and some no-so-public places. You didn't like the spycams but eventually got used to them. After all, you like to feel safe from unknown threats and you certainly don't want to pay the cost of someone else's shopping or any coworkers slacking off on the job. You often hear about abuses such as covert spycams in changing rooms but in today's highly charged

post-9/11 environment there's not much point in complaining. Nobody will listen.

Phase Two started just a few years ago, as continuing advances in wireless technology and miniaturization started placing tiny - but highly effective - multimedia devices in the hands of ordinary consumers. This new batch of users didn't need any large outlays of cash or any special training and some of them didn't feel that they should be constrained by privacy laws or any notions of propriety. This led to spycams being placed in all sorts of odd, intrusive places like residential bathrooms, clock radios, fake smoke detectors, and even the tops of shoes. Just google "spycam" and you'll see that there is a thriving industry based on this concept. In case you aren't aware of how pervasive or how capable spycams are these days, a good introduction is Marc Reesler's article "How to Find Hidden Cameras" at <http://www.letnatic.franken.de/papers/hiddencams.pdf>.

Modern technology created these possibilities but has yet to offer any inexpensive, easy to use countermeasures. Miniature radio frequency (RF) detectors are available from a few companies. For example, P3 International sells an inexpensive unit that they describe as a wireless camera detector. It certainly does work as advertised but it isn't effective in all circumstances. For example, try using it in an area with wireless speakers or close to a switch-mode power converter. More capable devices have been available for some time from companies like Optoelectronics but of course they cost more and require some expertise to use properly.

Camera phones are the most recent privacy threat. They're difficult to avoid due to their portability, tiny lens, and widespread use. Cell phone detectors are one solution but they're not cheap, and in any reasonably busy area they'll get nonsensical false hits from ordinary cell phone usage. You could just nuke all calls with a cell phone jammer but that's kind of risky in the USA and the many other countries where such devices are outlawed.

Enough history. Let's review what we have so far. Phase One was "Big Brother's" spycams in public places. Phase Two saw the introduction of other people's audio and video spookware in their shared places. The progression should be obvious. The next phase will bring common criminals' spookware into your own private places. The required wireless and multimedia products are already available and the robotics platforms aren't too far behind.

### A Simple Example: Burglary

Let's start with clothes dryer exhaust vents. As a general rule, they feed directly through the exterior wall into living space. How convenient. They're four inches in diameter which is large enough to accommodate all kinds of gear, and they're located low down on the ground floor (nobody wants to run upstairs or downstairs to do the laundry) which means that they're easy to access from the outside. It doesn't take any space-age tools to remove the outside vent cap, separate or cut off the duct feed, and then rock the dryer away from the wall. This deconstruction activity is likely to tick off Fifif big time but she doesn't know how to dial 911 and the alarm system's motion detector around the corner is clueless to the big happenings in the laundry area. If Fifif proves to be too much of a nuisance or if the clothes dryer is too difficult to muscle out of the way then a good alternate route is provided by the air exchanger. It has input and output ducts which are four inches or larger and typically lead to an unmonitored basement area.

Once the duct has been cleared the next step would be to shove through a Robots R Us BurglarBot and while it's unfolding, retreat to a more comfortable position to prepare for some leisurely remote-controlled burglary. Just like Fifif, the BurglarBot is too small to trigger motion detectors but large enough to climb stairs and jump onto countertops.

Okay, so there's no such thing as a BurglarBot. The best a burglar can do right now with off-the-shelf consumer gear is strip down a small RC truck, strap a perlight, wireless camera, and a custom gripper onto it, and hope that the homeowners keep their jewelry and other valuables on the floor. Not much of a payoff for a criminal act. But if you consider industrial equipment, there will soon be many more options available. Google "ventilation duct robot" and pay particular attention to the so-called micro units. You'll see that there are already several small, versatile robotics platforms for sale. Once they've been shrunk by another factor of two, the addition of a tele-

scoping arm will transform them into real security threats. As always, there's much better stuff cooking in research labs. It's usually aimed at defense or rescue applications but might some day find its way into your house. For example, the University of Minnesota's Digital Technology Center is developing reconnaissance robots the size of a soda can (google "COTS Scout") that can easily fit sideways through a clothes dryer duct. They can jump up stairways. They can assemble and transmit complete 360 degree panoramas of each room. Cool. SUNY's robo rat (google "robo-rat abc") looks even more dangerous: a cyborg that could eventually become a well-trained burglary tool.

Don't think that clothes dryer ducts are the only vulnerability. There are many other ventilation pathways into a house. Most of them are constrained by flooring, joists, and drywall, and are terminated by well-anchored equipment. But that doesn't make them much more secure. A determined burglar could easily reach into the hole in the exterior wall and cut through the ceiling drywall.

### Internal Interfaces

A separate concern: these other pathways lead to more active areas of the house which means that they're vulnerable to privacy intrusions. To better understand the possibilities you can start by examining one of your own bathroom fans. You'll need a step ladder and a Phillips screwdriver. The fan's grille is probably held in place by spring clips. Carefully pry it away from the ceiling - you'll notice that it doesn't take much strength to do that - and then release the clips to remove it. If the interior of the housing has an outlet and an electrical cord then the blower assembly is removable. Unplug it and loosen or remove any metal screws holding it in place. You'll see that the blower assembly doesn't provide much of a sound barrier. In fact, it probably has openings below the fan blades that are wide enough to accept a thin surface-mount circuit board. Look up inside the fan housing and you'll see that it has an exhaust port which leads to ductwork. There might be a lightweight spring-loaded damper just outside the exhaust port but it's not going to stop any kind of miniature robot and it's often too poorly sealed to provide any barrier to sound waves. In a quiet house, a microphone placed just beyond a poorly sealed damper can pick up conversations in the adjoining room, assuming that the bathroom door is open most of the time.

Looking down the road a few yards, consider a miniature "urban reconnaissance robot" that has reached the exhaust port and wedged itself in place. From there, it could fish a small cluster of three miniature cameras between the fan blades and the grille. Each camera would have its field of vision partly obscured by the grille but all it takes is some fancy image processing to blend the three signals into an unobstructed view down from the ceiling. And you thought your bathroom was a private place. Note that a robot this size is closer to reality than you might think: take a look at Robonomics (just google it), a tiny robotics research platform.

#### External Interfaces

So how hard is it to gain access to the fan's exhaust port? To answer that question you have to go outside and study some external vents - preferably the ones on your own house. You'll get into less trouble that way, plus you should have an easier time figuring out which rooms the vents lead to. Bring a flashlight. If you're the self-conscious type then you might feel strange while snooping around your house's external ventilation interfaces. You shouldn't. It happens to be a perfectly natural thing to do since it can provide answers to many questions that plague a typical homeowner. Questions like: "Why isn't my bathroom fan pulling air out?" "Where is that horrible stench coming from?" or "Why is there steam coming out of my clothes dryer vent?" Choose a suitable concern in advance so that you're ready in case one of your neighbors starts asking nosy questions.

You'll soon see that vent caps are often located in unexposed, out of the way places and so covert access is possible. They aren't considered to be particularly attractive so you usually don't see them in the front of the house where they might at least be protected by motion-activated lighting. Instead, they're on side walls or rear walls, possibly even further obscured by a foundation planting such as a conical cedar which of course provides cover for intruders.

There are two basic types of vent cap: louvered and hooded. Louvered caps are flush to the exterior wall and typically have four plastic louvers that swing out when the vent is expelling air. To inspect their ductwork all you have to do is raise two of the louvers and shine your torch in. Almost all ducts are three to six inches in diameter. Simple arithmetic (yup - divide by four) gives you some idea what you can stuff into there without damaging the lou-

vers. They're flexible when in the horizontal position so if you raise two of them you can get extra clearance at the center. Some specific examples: a four inch louvered cap is large enough to slide in a small FRS radio, a small Pocket PC or a AA battery pack. With some care, you could even squeeze in a mini PenCam. A six inch louvered vent can accept a D-cell battery pack, a Nomad Jukebox 3, and enough portable communications equipment to set up a remote-control command post.

Hooded vent caps are covered by an angled hood which protrudes from the exterior wall. They have a swing out damper to prevent backdrafts and to keep pests out. They might also have a separate removable pest guard held in place by hooks or snaps. Hoods that enclose a large volume can accommodate larger objects than an equal-size louvered cap but even the big ones are extremely awkward to look into. Standard flashlights don't fit (since you need to shine them straight in) and the wimpy ones that do fit don't provide enough light. Flashlights with small swiveling heads are more likely to provide enough lighting, as well as the compact disposable units with three side-by-side batteries. Unless you have a really odd-shaped head, the next challenge is to actually look inside. It's possible to position your head under the hood and use a small mirror but I wouldn't recommend it. Interpretation of a tiny reversed image while juggling a damper, mirror, and flashlight is not a skill that you want to acquire. What you need is a small video device which can be inserted and then interactively positioned, e.g., a PC camera.

If you live in a town house or some other multi-family building then don't forget to check for bathroom exhaust ducts which might pass through the attic to the shared (and hence insecure) rooftop. But don't actually go up on the roof. It's dangerous, and besides you can see more by going up into the attic. Just watch out for protruding nails and don't step through the ceiling. If there is ductwork up there you'll see that it's the flexible metal type and it follows a smooth curve from the fan housing up to the vent. Rooftop vents are the easiest ones to snake equipment into since their ducts usually don't have any sharp bends and also because gravity does most of the work. That makes them soft targets but not necessarily high value ones: what goes on in the bathroom itself isn't of much interest and an upstairs bathroom typically borders on high-traffic areas rather than discussion areas.

These are just generalizations - your house might be different.

#### Two Privacy Intrusions

So where in your house would you go to place a sensitive, confidential phone call? Assume it's about something really big: your strategy for the next football game, a plot to overthrow the mayor, or maybe the next release of your network sniffer (spelling intentional). That kind of deep thinking requires lots of beer or soda pop and other good stuff. So the kitchen is the perfect place. If it has a central island counter, the kind with a cooktop and integrated surface downdraft vent, then you might place the call from that counterpost. Well, if that's the case then there could be a microphone literally right under your nose.

Open up a cabinet door near the vent and you'll probably see a honking big six-inch duct coming up out of the floor. The microphone would be right there where it meets the integrated blower. Stove ducts are required by code - to be composed of rigid metal ductwork. It's stiff so it won't have any sags or bulges that are difficult to fish through. Since it's smooth there aren't many ridges to catch incoming or outgoing gear onto, although you do have to watch out for exposed sheet metal screws. Last but not least, downdraft vents need more pull than the overhead types so the ductwork has to be at least six inches in diameter. So downdraft vents are another soft target, as long as the duct isn't blocked by a remote blower or a pop-up snorkel vent grille.

Maybe you don't like to use the kitchen for sensitive calls because too many family members hang out there (your parents, your kid sister, your own kids, whatever). Then the basement might be a better location even though it's less well equipped. But if it has a bathroom bordering on the main area and that bathroom has an exhaust fan, then it might be less private than you think. You probably noticed its vent cap during your outside tour. It's located low on the ground so it's easy to access. But the ductwork consists of flexible metal tubing. It's corrugated, has lots of sags and bulges, and is thin and easy to damage; very difficult to fish equipment into. If it has any bends or if it runs for longer than ten feet then it's probably immune to the simple method that I'll describe in this article. But who knows - you might dream up more effective techniques.

#### Microphones

Now that you know where the soft spots are, the next step is to actually try planting a

microphone to measure its pickup range and see how vulnerable your place is. There are all kinds of esoteric equipment out there but I'll focus on standard consumer stuff so that maybe you can choose from your existing treasure trove.

Let's start with the mic. There are three important things to remember: First of all, you're trying to pick up far-field signals so don't use a noise canceling mic. Secondly, choose an omni directional unit since its orientation will be hard to control. Thirdly, use a wired mic since they're small, can't be picked up by RF detectors, and also because the wire makes it less likely that you'll lose the @#%\* thing deep inside a duct run.

If you're testing with a PC then a small multimedia mic is fine, otherwise use either a tie-clip mic or a lapel mic. The classic tie-clip design's tiny mic and separate battery box make it ideal for covert recording in public (it can even be fitted into the top of a disposable pen) but the small size reduces sensitivity a bit and the separate battery box is yet another bulge that might get caught on a sheet metal screw or whatever. Lapel mics are more compact as a whole because they integrate the battery box to the microphone housing but they're also more likely to have a modern right-angle plug which is less than ideal - you'll see why soon enough.

The recorder should be placed just inside the vent cap so that the cap's louvers can be fully closed to block outside noise sources. The mic's wire probably won't be long enough so use a headphone extension cable but make sure it's shielded and is a straight cable, not the coiled type. Get the minimum length you need - shorter is better. Headphone cables have three conductors so they're perfect for stereo mics or PC mics and are also usable with the mono mics used by most portable audio gear. I hope you know not to plug a PC mic into audio gear or vice versa - they aren't compatible.

#### Recorders

Even if you succeed in positioning the mic right next to the fan's exhaust port, its location guarantees that the signal will be muffled and reverberant. So the ideal recorder would have continuously adjustable microphone sensitivity that you can crank up to an abnormally high level. It would also have digital outputs so that the audio can be uploaded for further amplification and more sophisticated enhancement, and of course it needs a jack for an external microphone. All portable dictators and some minidisc recorders have those features.

They're good test tools but don't have enough recording capacity for real-life surveillance applications. Another possibility is an MP3 recorder with a line in jack but it would need a preamp to raise the mic input to line levels. I don't know of any small off-the-shelf preamps so you might have to build your own: look for "audio preamp" at sites like discover-circuits.com. Keep away from phono preamps - they're special-purpose devices that were used in the last century when music was recorded on vinyl. Note that the Nomad Juicebox 3 has a line in jack, or google "line mic recorder" to find a smaller unit. Try to get a model that can record raw audio without compressing it.

You might think that a pocket memo recorder would be perfect for the job. For example, the Olympus DS-330 Digital Voice Recorder is the size of a cigarette lighter, lightweight, all-digital, and has a jack for an external microphone. In standard playback mode it can record two hours and thirty-five minutes which is more than enough for acoustic testing. But it doesn't have enough dynamic range for most surveillance applications: it only has two sensitivity levels, and its aggressive compression algorithm reduces low-level speech into low-level incomprehensible babble. So it's only useful in ideal conditions: fans that have no exhaust port dampers and are close to the target area. An extra pre-amp stage might help.

A notebook PC makes an excellent recorder - see my article "Microphones, Laptops, and Superaps" in 20:2. Configure it for 16 bits and either 8 KHz or 16 KHz. A Pocket PC or PDA is even better, as long as it has a jack for an external microphone. Just use whatever you have - even a boom box with a cassette recorder is good enough for exploratory tests. But remember that a real intruder will probably have better equipment than you do. Don't assume that battery life is a serious constraint. It's easy to hook up external battery packs. A homemade microphone cable could supply endless power to replace the mic's tiny button cell and as an added bonus it could supply a higher voltage to boost the mic's sensitivity a few dB.

**Installing the Microphone**

The ideal microphone delivery device would be some sort of robotic "duct rat." You probably don't have one lying around in your toolbox so you'll have to find some way to fish the mic into position. It might be harder than you expect. Take interior measurements first

so that you'll know how far the mic has to be inserted. If the vent cap is hooded don't just fish blindly assuming that the ductwork is all in a straight line. The location of the vent cap is constrained by clearances to the ground and to windows so the duct might need a downwards twisting drive to get lined up between the joists.

If you want your test to be realistic then you'll have to use unobtrusive equipment to insert the mic - I doubt that an intruder would go skulking around your neighborhood armed with duct cleaning brushes. Try to find something smaller. Whatever you do, don't use an electrician's fish tape - they're much too stiff and are sure to damage unseen flexible connections, the damper, or the fan blades. A metal tape measure is stiffer and is a lot more convenient to carry around. A slim, lockable 16-foot unit with a removable belt clip is a good choice since you can insert it into the vent cap once the mic has been positioned. Go to a larger size if you need more stiffness or length but then you might have to leave it outside the vent cap and the louvers won't be fully closed.

Attach the microphone with masking tape so that it will be easy to release once you're done. If you're using a lapel mic then tape it facing down just beyond the end of the measuring tape. If you're using a tie-clip mic then let the mic element extend an extra half-inch so it can hang downwards. Use plastic-coated 18 gauge wire to fasten a small plastic cat toy (the kind that comes with a bell inside) over the end of the measuring tape. The cat toy provides a protective cage for the mic and prevents the metal tab at the end of the tape from catching on things. Don't forget to turn on the mic. If it has a separate battery box then tape the box into the curve of the measuring tape. Position it to protect the on/off switch or if that can't be done then cover the switch with a piece of masking tape. You also need to tape down the join to the extension cable and that's when you'll realize that an old-fashioned straight microphone plug is more appropriate than the newer right-angle ones.

Pay out the measuring tape from a distance of two or three feet so that you can accurately gauge dependability. Measuring tapes are only flexible in a single plane. If you're fishing into rigid duct that has a vertical bend further in (typical of downward vents) or flexible duct with vertical sags then orient the tape as though you were measuring a floor. If you're fishing into flexible duct which zigzags within its 16 inches of joist space then hold the tape

measure sideways. Let the tape pull in the mic wire. If the wire stops pulling in it means that the tape has gotten folded over itself which isn't good. Reel it back in and try again.

Once you've got the mic in place you can congratulate yourself: you planted a mic deep within the bowels of the house and set up a recorder in a weatherproof, easily accessible location. You did all this from the outside without being detected by the alarm system. But before patting yourself on the back too hard you should check if the setup is effective. Go to the target area and place a telephone call or speak as though you were in a meeting. If the pickup isn't what you expected then remove the blower assembly and check where the mic actually is. It could be in the middle of nowhere, right on top of a particularly noisy A/C duct.

**Epilogue**

So that's it for Duct Fishing 101. You might be wondering about the other vulnerabilities I mentioned earlier, like chimneys and sewer

lines. Well sorry but I'm not about to put my equipment in those places so you're on your own. But if you're expecting robots to come bursting out of your toilet like the creature in *Alligator* (1980) then forget it - that won't be happening for the next decade or so.

If you're like most people then you don't leave your valuables on the floor, and you don't hold secret meetings that anyone in their right mind would be interested in. So you won't lose any sleep over this article. If you wake up late one night to the sound of someone's voice coming out of a nearby bathroom fan, don't be too alarmed - it's just some doofus who's decided to sacrifice a cheap FRS radio for a practical joke. But be more wary if you wake up to strange, inhuman noises radiating from the ceiling. Pulsed, high-pitched whirring sounds characteristic of step motors or precision servomotors, maybe even miniature high-speed cutters. By then it will be too late. Maybe you should go out and look at those ducts right now....

# A LESSON ON TRUST

by Sairys

While I can't say I'm very proud of what happened, it does show a certain truth of the computer world. Hackers (using the term lightly) do not stick up for each other when things take a turn for the worse.

During my junior year in high school, the school network security was a joke. The school admin's goal was to block student access from the C:\ drive, prevent us from obtaining DOS access, restrict us to our username folders, and block us from inappropriate web sites. I'm sure that the school faced security issues before but they did nothing to make it more difficult for us.

Being a typical student, I wanted access beyond what the web proxy would offer me. When class got dull I took refuge in a quick game of Slime Soccer or Jet Stalom. As these sites became more popular and the proxy started picking them off one by one, alternate

ways had to be found. I soon discovered very apparent things people would not check for: the initial ASCII URL. If a student came through an IP address, the proxy did nothing. Over the span of a month, the school switched proxies about three or four times. They finally stumped us with BESS. So far the only method around it is to use Babelfish to translate websites back to English (although now they block AltaVista as well). Also, sometimes it misses websites that have a www2 clone of itself. The most outrageous thing was when www.google.com was blocked, but after enough complaints it was once again cleared as an appropriate site.

At the time I was also enrolled in a computer science class, a CISCO networking class, and an A+ tech class. Each of those classes had use of the command prompt. Doing labs where one needs to ping a machine or run tracer across a network is impossible



when Altiris is blocking you. After a few days of watching the teacher do the labs for us on the overhead, a few of us realized that Altiris only blocked the command prompt from the start menu. A quick glance at a Windows 2000 install showed that the command.com file is in the C:\WINNT\SYSTEM32 folder. The best thing was that Altiris did not prevent us from making shortcuts. So a quick link to the command.com file gave us the prompt we dreamed of.

At this point the wanna-be hacker inside a couple of us woke up. We began to have a bit of a game going. See what you can learn about the network. I must admit that it was fun and even exhilarating. A week later we already had access to the C:\ drive and command prompt access. We learned that while Altiris would prevent us from entering local URLs by hand, it had no issue with links. So a simple hyperlink to file:///C:\ would give us the drive. From there we could run command.com, telnet, or anything else that we wanted.

Until this point it was nothing special. A little bit of clicking and some short HTML. Eventually an accomplice of ours learned a teacher's password. None of us worried about using it because we still didn't have grade-book passwords, nor did any of us desire them. Teachers have it a little bit easier than students. At the time, teachers had full access to student folders. Also, they had no restrictions of the command prompt and could even execute regedit. Nevertheless, the key was when we saw a small login script executing in the background. We took a screen shot and found the location where the file was being run from. It was this file that made me aware of the array of "net" commands. "Net use," for example, will map a network shared directory to a drive letter. That's how the servers automatically displayed the O:\ drive for students and the T:\ drive for teachers. Also, I learned about the "net view" command, which displayed all the computers on the local workgroup. When I ran this command, the results were astonishing. Every machine in the entire school district was visible from any node. Using the teacher account, I could "net use" to the folder of any student that belonged to the school district. Be it a middle school kid or the prom queen of the rival high school. While this was "cool" at the time, it was of no use to us. The

thing which to this point amuses me is that the admin of this network created a master login script for himself. This script would automatically "net use" to every directory on the district server. This still did not do much. At this point we had access to every student folder, but were still restricted to the single teacher's files.

It was by pure accident that I struck gold. A class of mine went to one of the computer labs to type up some essays. I picked a computer and powered it on, but was welcomed by a blue screen that claimed the boot volume to be corrupt. Needless to say the computer wouldn't work. Being too lazy to shift a computer over I tried to see if I could get to the command prompt and run anything to fix the problem. I was unsuccessful, but once the class left the room for lunch I found myself alone with the machine. Actually, I was desperate for results so I began looking closely at the boot prompts: "Press F2 for diagnostic" was one of them and it seemed appropriate at the time. I hit F2 and was greeted by a Boot works logo. The available options were all grayed out so I couldn't do anything, but when I quit I found myself face to face with the command line. It was time to explore.

DIR showed a file called startnet.bat. They couldn't have made this simpler. This file called all the necessary programs to connect me to the local network. Better yet, no login needed. Once I realized that I could see other computers, I checked to see if I could access my personal folder. I could. Using "net use," I mapped the teacher's directory and found I could access any folder I wanted to anywhere in the entire school district server. I also quickly learned that every machine was, by default, sharing \$C:. This meant that remotely I could access the C drive of every computer. At this point I should have reported this hole to the admins and saved myself the trouble, but curiosity got the best of me. This was too good to be true. There was almost no way to trace who was at the computer. There was no username, no password. The only evidence would be IP information and MAC address, but since hundreds of students sit in that lab during the day, it would be hard to trace it back to me.

Another check at the network computer made me laugh a little more. TROY PROXY was the name of the machine which housed the friendly BESS guard dog. A simple DEL

statement would get rid of it all. Fortunately, none of us had malicious intent. At this point, the network was at our disposal, and even though there was nothing we wanted from all those folders, it was sure nice to know that they were available to us. It was like being released from a prison. Also, up to this point no one had any idea what was going on. None of the admins even bothered to check up on the red flags that were probably showing up on their systems. Nevertheless, the fun had to end at some point.

A certain student who went by the alias eCKO decided to play some more games. He learned how to remotely shut down machines, as well as eject CD-ROMS. Personally, I was a little intrigued but he decided not to share this information. Anyway, his fun backed off on him. During one of his classes he began to eject his teacher's CD-ROM from his computer. The sad thing is that he admitted to it personally. He claims to have thought the teacher to be "cool" and not rat him out. *Wrong!* Within a day, his username was blocked. This posed problems for him since he needed to get to his student folder to get some files. He got the bright idea that since he knew a teacher's password that he would simply use that to get his files. Needless to say, his computer was being watched. The moment he logged in with the teacher username, his computer froze as the Altiris "eye" watched his screen. He knew he was busted.

It took about two days for him to turn himself in. He admitted to using the teacher password and claimed that I had given it to him. I quickly got a pass to get down to the office and was interviewed, prison style. As I sat there I heard a few other familiar names getting called down, and saw a few familiar faces pass into a nearby "conference office." It was clear that everyone who was in on this was rattled out. I did the only thing I could and tried to save my ass. There was no denying the fact that I used the teacher's account and accessed data that was not mine to access, but no harm was done. I figured that as long as I told the technicians how to fix their problems that things would be all right.

Into the second hour of the meeting, two computer techs walked into the room and decided that they wanted to talk. I told them about all their security issues as well as the major Bootworks flaw. I can honestly say that they were decent people, one of them at least.

We cracked some jokes and in the end they decided that since I personally did not cause any damage that they would talk to the principal and get me off the hook. "According to us, you're not in any trouble." Great words to hear at such a moment, but unfortunately they were empty. They did speak to the principal, but she claimed that some action still had to be taken. All four of us were suspended indefinitely and we had to schedule a hearing. We all got our sentences on Friday, but I was fortunate to get a hearing the upcoming Monday. The meeting was pointless though since my statement meant nothing to the principal who seemed only concerned about us gaining access to teacher e-mails, which we did not do. Either way, two of us got a week's vacation, the kid who originally got the password was out for an extra day, while eCKO was out for two weeks and lost all of his computer classes. Also, he didn't receive a very warm welcome when he returned.

Someone once said "If you tell anyone about your acts, you've already made your first mistake." Probably the best advice one could offer. Trust no one. While you think your friends will not rat you out, just wait until they sit in the hot seat. Also, as far as school "exploration" is concerned, keep away from it. While most admins will not concern themselves too much, the repercussions could be serious. While suspension is not very bad, especially since the absence is exempt, worse things could happen. In eCKO's case, he lost his computer classes. But if anyone suspects tampering with the gradebooks, your own grade could quickly become void. Imagine trying to send a transcript with a note that says your grades are invalid. We don't like the message "Invalid" on our computers, let alone our high school transcripts. I was fortunate this time, but it took me a few weeks before I got back on track with all the schoolwork I missed. Also, as expected, my grades dropped a little in all my classes. I have decided since to leave the school computers to be used for their intended purpose. As for the admins, they ghetto patched some of the loopholes and completely ignored others. "Sources" claim that the DOS access no longer works and simply displays an empty directory. BESS is still at large, but we still have our shortcuts.

Continued from page 39

A) Steals computer services

B) Steals a company's products through a computer-based ordering system

C) Illegally copies and sells copyrighted software

D) Attempts to gain unauthorized access to a computer system

Obviously, I wouldn't be writing if I thought a correct answer was among their selection, but there is not. Yet another unfortunate example of the misrepresentation of our community.

spahall

You're not going to tell us which one was their right answer? Actually, it seems odd that someone with no understanding of hackers wouldn't assume we're guilty of all of these. Equally odd that someone who did understand hackers wouldn't have an alternative answer. Are you sure there wasn't an "all of the above" and/or a "none of the above" choice included as well?

Dear 2600:

After reading all the letters about insecure systems in the previous issue, I wanted to write to you and share the wonderful experience that I had in setting up my voice mail at school this past year. I go to Rensselaer Polytechnic Institute (www.rpi.edu) and everyone who works there is stupid beyond belief for a number of reasons. One of those reasons is the handling of the voice mail system. In order to initialize your voice mail you have to pick up any phone on campus, dial the voice mail number (6096), then dial your phone number (for instance, 4002), then input the default password (123456), then use the means to enter a real password, set your greeting, etc. The problem with this system, as I'm sure you've already guessed, is that anyone can set up anyone's voice mail. When I first set mine up I accidentally dialed the wrong number and set my own password and greeting to my neighbor's phone. I could easily have gotten to school a day early and set every voice mail on campus to profanity or something equally juvenile and damaging. The point of this is many large organizations like schools and corporations seem to go instantly stupid when issues of security come up. The fact that voice mail exists is apparently good enough for them. Any concerns about security or impersonation are just ignored.

ManicDm

Even 20 years ago this would have been considered absurdly dumb. But we're impressed that they deviated from the 123456 default password string. We smell a Durrwin Award.

Dear 2600:

Hi my name is Ashmit, I guess you already know that lol. Anyway, I got your e-mail from the www.2600.com website. The reason I am emailing you is because I was hoping you could help me out with a little something. I need to know whether you can gain access into a web server and its database. If you can then we are set. Basically here is the deal in a nutshell. I need someone with the abilities to get into my school server and change a few things. I have saved up \$3900 over the past year for this and am willing to pay it in cash, as I am from the Washington area. You do not have to worry about getting caught because I am sure as long as you erase your tracks, there is no way of either one of us being caught, guaranteed. I

hope you can help me out because I am extremely desperate.

Ash

"Desperate" doesn't begin to cover it. Whatever your problems, and we certainly won't try to minimize them, they are nothing compared to the world of hurt you'll enter if you do stupid things like offer complete strangers money to help you do illegal things. But even if you weren't a complete stranger we would tell you the same thing. And just where did you get this distorted view of the hacker world where this is the kind of thing we do? Yeah, we know - the mass media. It's still no excuse. There should be something in your genetic code that alerts you to the fact that you're doing something extremely stupid and wrong.

So we're clear, the offer was in Canadian dollars and not American, right?

Dear 2600:

From Verizon's public website under "Local Phone Service," "Online HelpFAQs," "Voice Mail," you will find instructions for "Getting Started with Home Voice Mail." Step number three says: "Dial your starter password, which is your seven-digit home telephone number."

So basically all you have to do is find someone who has new service or someone who has not changed the password and you can own their voice mail. Theoretically, you could take Verizon White Pages from last quarter, compare it with this quarter's and find all the new customers. Then you could just punch in numbers from the Verizon White Pages until you have a hit.

Just to further test their security on this I called customer support (and not from my home phone) and claimed that my voice mail was locked out. They changed the password for me. All they asked for was my name, address, and home phone. No account number, no Social Security number, no "amount of last bill," mother's maiden name, or any other verification questions. Thanks Verizon!

The Great Beltzoni

Dear 2600:

This is an update to the "coupon trick" article printed in 2002. I was so intrigued by the article that I immediately began making up some coupons for a test run at a local department store chain called Fred Meyer. Like any had recently installed self-checkouts and was eager to see if the trick worked. Well, it did work but I found myself wanting more. In the original article the author discovered that a 30 cent coupon that the numbers 3030 in the barcode and that by changing them to 7575 that his bonus was instantly a 75 cent coupon. The problem is that his basic method is limited to a cents amount, or a maximum of 99 cents. I wanted to make up coupons worth dollar amounts. After clipping every coupon out of the Sunday ads I compared all of the \$1 coupons and all of the \$2 coupons and so forth. Well, it was very easy to figure out that all of the \$1 coupons had the exact same code as each other and all of the \$2 coupons had the exact same code as each other and so forth. I searched for the coupon with the highest value and ended up with a \$3 coupon for Crest whitening strips. I merely wrote down the two digit code used to represent \$7 and applied that code to a coupon I had for a box of Tide laundry detergent. I printed up the

coupon and used it on an \$8 box of Tide and sure enough it subtracted \$7 and gave me a grand total of \$1. Happy shopping and enjoy!

Chit

Let's once again make it clear what the difference is between hacking and stealing. Discovering the vulnerabilities, figuring out the system, and testing it are examples of hacking. But you seem to have walked over to the vending community which really doesn't involve much in the way of skill and simply turns you into a dishonest person. And don't try to use the "right price" logic as the people (most likely in the store) who have to cover the difference are probably a lot more innocent than you. We only ask that you do us one favor. When you get caught and prosecuted, don't go telling the authorities that you hacked the system. All you did was mess around with one part of it in a very crude manner.

Dear 2600:

We need more magazines like yours with an otherwise unseen view on today's media community. I'm writing because I have a problem and wish to complain (not about you but to you). Maybe I can get a few suggestions as well. I'm 18 and live in a residential program for "troubled youths" in Massachusetts. I rarely have access to a computer with internet capabilities and when I do it's for a very short period only. My main hobby is computer work and hacking. But my lack of access to a computer drives me crazy. At home on the weekends my one refuge was my broadband connection through (thech) AOL, no less. Now even that has been taken away and my camp time is more limited. School computer usage is limited in itself to researching colleges or a Mac.

I was so excited when last year the program said we'd get a laptop and internet access. I found out that our pal Mr. Gedge had fallen asleep counting his money again and our internet Explorer was corrupt. When I went into the Network Neighborhood, surprisingly to me, the installer for MSIE was in the same folder as a directory of private patient information - unlinked!

I notified our computer guy who handed off the info to someone else who interrogated me as to my "hacking" into patient files. I had stumbled onto a directory, not opened it, and notified the admin at once that sensitive patient data was notified. Now the admin (who's a bit of ainker himself) didn't have the brass to own up to his mistake and he let me take the heat.

It's funny that a year later that same guy has given me the only admin account to our new computer (no internet of course).

Hell, I can't even get a subscription to your mag because my dad works with anti-terrorism and isn't sure what people would think if 2600 came to our house!

Homeland Security

There are two points that stand out dramatically in the lines of the recent local Department of Homeland Security

"Town Hall" meeting. First is the fact that this meeting was held at a private school. Why couldn't this meeting be held in Seattle's Town Hall? If the security of the city's public buildings can't be trusted, then isn't that an important topic for discussion? This issue wasn't raised by either the Seattle Times or the Post-Intelligencer.

Second, I walked into Campion Hall two days ago and picked up an eight page stack of paper lying on a desk titled "Seattle Town Hall Attendees." Several copies of the document were laying on the desk and had various names checked off, none of which were labeled as confidential, restricted, or sensitive information. Further, the copy I put in my backpack was next to a stack of brochures. I was being watched by several police officers and a few men in suits who I assumed to be DHS employees. None of them attempted to stop me from taking this list. On later review, the list is a four column table which may have been derived from the web sign-up form. There are columns for First and Last Name, Occupation, and Title. The list is sorted by last name and some of the fields are blank. Some of the names are initials and they appear to be people of some import, which leads me to speculate that they would be ushered through without being closely questioned or searched (although I wasn't there in time to witness the ingestion). Close examination of the document reveals that Tom Ridge is not on the list. Neither is Steve Ballmer, who was in attendance according to various news sources. This gives me the impression of a separate class of VIPs who were not required to register and be screened by the DHS. I do not intend to publish this list of names; my point in taking a copy was merely to illustrate the lax attention to detail and disregard for personal privacy in the Department of Homeland Security. However, for purposes of verification I will share this excerpt from an attendee named John who wrote in the "Occupation" field: "Please don't draft me."

If this is an indication of the level of privacy that the Department of Homeland Security intends to provide, I do not support it.

Lee Colleton

Dear 2600:

This is in response to an anonymous letter in 2004 about Department of Homeland Security regional offices (disguising themselves as other government offices). As far as I know, DHS doesn't have many regional offices and, of all government agencies, the only agency that disguises itself as another government entity within this country is the CIA (it seems that CIA domestic offices are commonly disguised as the Secret Service). DHS, I believe, does not employ anyone directly outside of Washington. Instead, what people like to think of as "DHS agents" are really officers of its component agencies, i.e., CIA, DIA, FBI, NSA, etc.

Prospero

Redirecting

I have a lot of respect for everything you have done to ensure that cyberspace remains the last enclave of free speech. I have a lot of respect for your continued fight with those that would like to own, control, and sell the Internet. But you are dead wrong on the hackergangster

from.com issue. I believe that no one has the right to point his own DNS entry into someone else's website. Why? Let's imagine that you have a family website with your wife's and kids' pictures and a family register (family-trial.com) which then points right to your website. Would you like that? Would you like that fuckmaterial.com site advertised on all the available search engines? Would you like the resulting e-mail directed to your family? I do not think so. A byproduct from a website pointing to another website is a different story, but advertising a website that purveys points to someone else's material, copyrighted or not, does not seem right nor fair to me at all.

**Steve Duch**

What you suggest runs counter to the very foundations of the net and flies in the face of free speech. No, it's not very nice and yes, some people may get offended. But it's far more offensive to us to be told that we are not allowed to make a statement or to be told that we cannot redirect to a site without permission. And your fictitious family scenario is easily dealt with by simply denying any connections that originate with the offending site.

### Observations

**Dear 2600:**

I just watched the documentary called *Freedom Downfall* and was blown away that the government of the United States was able to break its own laws and not be brought to justice. You've probably heard this over and over again for the last few years plus, but it's new to me, and I just wanted to let you know there are still eyes being opened.

**Mugford**

Thanks for the feedback. Be sure to check out the DVD for even more eye opening material.

**Dear 2600:**

I have a Nokia 3390 with T-Mobile as provider. When I put my phone in silent mode and vibrate alert is off, if someone calls me from a land line I can hear them talking before I answer the call through the earpiece on the phone. I discovered this recently when I had my phone set to silent mode and vibrate alert off. I heard my friend's voice saying "pick up the phone, pick up the phone" and my phone was displaying "incoming call" before I even hit the send key to answer. The sound is not as loud as it is in a normal conversation, but still this is very interesting. If someone calls me from a cell phone this does not seem to work, only from a land line phone. I am not sure how this happens but consider it deserving of more research.

**Pablo**

We've gone nuts trying to test this out, although not on your specific model. So far no luck. But it's not the first time we've heard of similar occurrences. No doubt our readers will have more to say on this.

**Dear 2600:**

I am a Terafone user and have been for some time now. Overall I have been pleased with the service I have been getting. However, as I was trying to add minutes recently, I noticed something sinister. I went through the usual automated menu nonsense, but when I got to the part where I was prompted to add my minutes, I was asked to make up a PIN. This has never happened before

but my problem was when the prompt asked for the PIN to be the last four digits of my Social Security number. I called the Terafone people to see why. I got the line was expiring, telling me I had nothing to worry about, this has nothing to do with the government, and it's only for customer service purposes. Yeah, like if Big Brother is your customer service rep? If the number is only for customer service reasons, why ask for the Social Security numbers in the first place?

Just a little heads-up for everyone.

**Michael J. Ferris**

Did you try simply not giving it to them? If they don't already have it, there shouldn't even be an issue. But if they would have been back when it was originally given to them. Unless there's a credit check involved, you can get away with giving them a fake number. Obviously, you don't want to lose track of the number, you've given them or things could get very complicated. From their point of view, this is a better default password than 1234 since it's about always unique for different customers, but still easy to remember. But if they're suggesting that everyone use the last four digits of their Social Security number as their normal PIN, that's a very bad idea for obvious reasons.

**Dear 2600:**

Stephen recently noted (21:1) that US soldiers are "to be in the mindset of being deployed at all times, be it at home or abroad" and that reminded me of something from Aldous Huxley's *Brave New World Revisited*, end of the first chapter:

"But liberty, as we all know, cannot flourish in a country that is permanently on a war footing, or even a near war footing. Permanent crisis justifies permanent control of everything and everybody by the agencies of the central government."

Given current polling data, this was on a noun (terror) seems to me to be an awfully effective way of justifying permanent control without the messiness that was the Florida recount of 2000. I wonder if Congress and the States will repeal the 22nd Amendment so Bush can run for a third time in 2008. Or will they save everyone the trouble and just make George the King of the new United Kingdom of America?

**Michael**

Let's not get ahead of ourselves. 2004 isn't over yet.

**Dear 2600:**

I just came across this article with the following quote from John Kerry: "Have you had a beer with me yet? Like to have fun as much as the next person, and so on and back around and have a good time." I made the wonder if Kerry is a hacker in disguise. Maybe being a Massachusetts senator (hence of MIT) did him some good.

**antiope**

That was actually a coded message. We doubted that he was using the word "hack" in a public statement as a gesture of good will towards the disaffected hacker community. Bush has yet to respond to our demands. But we probably shouldn't be telling you this.

**Dear 2600:**

In response to @ehp0th's letter in 21:1, "Using a public form on a website to broadcast vulgarity hardly

accuses like 'hacking' to me" either. It was just a lame, juvenile pink that screwed up a free and potentially useful service. This sort of behavior is, by @ehp0th's own definition, not hacking, and not even security-related (as there was no security to defeat) and therefore out of the scope and below the quality level (in my opinion) of this magazine. I would ask @ehp0th and others to focus their time, talents, and energy on more productive works.

**Bryan**

Isn't this exactly what the writer already said? Why is it necessary to lecture someone who already agrees with you?

**Dear 2600:**

I have just read most of what happened at Pentagon Mall with the Secret Service. In Arlington this is nothing new. I have lived here for all my life and have been arrested for erroneous behavior like "Obstruction of Justice" while trying to walk away from an Arlington County police officer who was harassing me in a movie line at Ballston Common Mall (also in Arlington).

The clandestine actions of watching young tech savvy adults and teens by the FBI, the Secret Service, and mall police is really a waste of time and money. If they want to know what is going on at our public meetings then let's invite them to sit down and listen with us. We have nothing to hide and we are definitely not terrorists.

Furthermore, what in the heck were you guys doing with contraband in your pockets at a meeting? A meeting on guns and girls, this is not good. We have to give them no open reason to want to search us. Next time, please be someone to find a dub bag and have everyone get charged with dealing pot, do we? Like I said, let's invite a member of the Secret Service or the FBI (tech savvy only) to sit in on one or two meetings so they can see that we are merely intellectuals who enjoy solving problems and finding problems to solve.

**DRABZ**

Our meetings are always open to the public and that includes people who are part of law enforcement. We don't specifically invite people from any organization. As for the fears of the meeting attendees back in 1992, we certainly can't fault people who were worried about how certain things could be used against them. It's actually a very rare thing to find people who have absolutely no fear when facing such a formidable adversary, doubly so when you infect concerned parents into the equation.

**Dear 2600:**

First, I found a VoIP program called Skype. Excellent sound quality for free long distance calls. After doing a search (especially ages/sex), I found a few people online who were using their real names as usernames, first and last. So I started chatting to one girl and mentioned I was in college. She responded, "My brothers are in college and when I asked where, she told me. So I googled the school name. Found the college's site, ran a search for her last name (which wasn't a common name), and found both brothers with info they probably didn't know was public: name, phone number, major, academic year, *home address*. So I asked her if she lived at that address and of course she flipped out. The lesson here: Don't ever use your full name as a username and be sure to let the col-

lege admins know this sensitive info is available to any psycho with an Internet connection.

Second, I have recently discovered Live Unix CDs. They are full distributions of Unix that boot and run the entire operating system off the CD. The benefit (which I am still exploring) is that you can pop in the CD on a computer that requires username/pw login (i.e., campus computers) and reboot, set the BIOS to boot from CD, run Unix off the CD, and have complete use of the computer! When you are done, just reboot because everything was done in memory and there's no trace you were there! Just don't forget to grab your CD before you leave. Check out Knoppix, PCLinuxOS, SLAX, or PHLAK which have extra goodies.

Keep up the fight for our freedoms. It is from reading your great publication that I became active with EFF. **Cyosomany@khal**

**Dear 2600:**

I found Spud's letter in 20:3 about the FBI's presentations in Phoenix interesting since I also saw a similar presentation several months ago (set up by my employer). I disagree, however, with Spud's assessment that the presentation lacked "real world knowledge" or that it was all about a repressed fear of lack of control. In fact, I would argue quite the opposite - for what is truly going on here is a total hijacking of the hacker ethic by the authority that formerly sought to suppress it. While I found it rather amusing (on the surface) that the FBI increased heavily on 2600, the most chilling aspect of the whole thing was the overall message to my employer: when it comes to cyber-crime, the FBI can't help you.

The FBI agent doing the presentation made the point that security starts on every desktop. 2600 has been saying this for years, has it not? Now it seems your message has finally gotten through to the FBI. According to this presentation, the FBI's strategy to fight cybercrime is something called "information sharing." They have set up a network of organizations intended to work together, sharing knowledge of security flaws and weaknesses. The whole idea revolves around prevention and enabling corporations and those "at risk" to take their fate into their own hands - to arm themselves with knowledge. And yet, hasn't that been the point of 2600 from the beginning?

**Simon Shadow**

**Dear 2600:**

I would like to address two letters that appeared in 20:4. One reader was bothered by the use of the color black being associated with evil or bad. He also stated that while people commit most of the crimes, the facts support him only if he's talking about white collar crime. Perhaps in fairness he'll work to change the phrase "white collar" as part of his crusade as well. Another reader worried about the government knowing they subscribe to 2600. If you think the feds find you interesting, how about subscribing to the *Washington Report On Middle East Affairs* (pro-Palestine) or *Small Arms Review* (military guns and stencils). Visitors to Barnes and Noble really need to check out the complete history. Well, I have to go now. I think I see the Homeland Security Prize Patrol van pulling up out front. Maybe I'll be in their next commercial!

**Greg Gowan**



# How

# With

# Netcat



By **MobiusRenore**

The following is a presentation of a very useful network utility. Some call it the Swiss Army knife of network utilities. With it you can connect to a port on a server, listen on a port on your local machine, set up a backdoor on a machine, or port scan someone's box. The uses of these and other features will be made clear shortly. Standard disclaimer: This article is knowledge and is therefore inherently neither good nor evil; only what you do with it decides that. I cannot and will not be held responsible. That said, let's move on.

The first thing that I did with Netcat was to connect to a server. The typical command line options I use are "nc -v -v <server name> <port number>" (the double -v gives you an ultra-verbose mode). You can attempt to connect to any port, but only a few ports will be useful to us, specifically POP3, SMTP, HTTP, and a few other random ports.

After finding a copy to download (nc1int.zip for Windows or nc10i.gz for \*nix users (usually includes source files)), go ahead and connect to a web server on port 80.

(On a side note to those who must use a proxy server, Netcat is made simple with proxies; just connect to your proxy site in the normal manner in which you would connect to any other computer (including the port number of your proxy, of course) and when you issue one of the following commands, use the full URL of the site you wish to retrieve.)

Once connected it will list the server's name (e.g. google.com), its IP address, the port number, the name of the port, and open, with a blinking cursor at the end, waiting for input. This is the part where we get to explore HTTP protocol. By sending a GET request via Netcat, we can get the source code for the webpage. This is typically no big deal, unless it's one of those annoying pages that try to disallow you to see its source by disabling

right-click. The listing will scroll extensively if it's a decently-sized web page, so you should redirect output from netcat to an ASCII file. Now you have a copy of the webpage's source. Big deal, right? It gets a little more interesting.

The typical request is formatted "GET / HTTP/1.0". The slash is, of course, the root directory wherever you connected, where the index page will be returned if you didn't specify otherwise. You can change this using either absolute or relative URIs with usually the same results. Absolute references will typically work with the most accuracy. This is the typical request that your browser sends when it connects to a web server but without all the fat.

GET also works with images. For example:  
nc -v -v www.google.com 80  
>logo.gif  
GET http://www.google.com/images  
/logo.gif HTTP/1.0

This will give you logo.gif. All you have to do to look at it is to remove the http header from the file with your hex-editor (another essential tool).

Let's say now that you have a website with a form and you want to know what kind of information that it's going to post, wherever it's going to post it. Using simple javascript in the address bar of your browser (in Internet Explorer, at least), you can change the value of the action variable of the form. I suggest setting up Netcat to listen on a certain port while changing the action of the form to something more suitable like "http://<your ip address>:<portnumber>". (Hint: if you're behind a firewall, simply use a common port that won't be blocked [80 works for me]).

After entering your javascript, submit the form and wait. Netcat should print some information, at the bottom of which is the information in which you may be most interested. There will probably be a "content-length = <num>", where <num> is the number

of characters submitted by the form. This is important, because you're going to copy this information in a text editor in order to have some fun with it.

You can alter the information that it was going to post, as long as you change the content-length field above to reflect your changes. You can delete some of the other fields as well, but depending on where it's going to be posted, you may need to keep those fields the same as when you received the form.

After editing the form-submission to your taste, start up netcat again, but this time use it to connect to the server from where you got your form data. This time, instead of doing a GET request, you replace GET with POST. The full command will basically be "POST http://www.google.com/search HTTP/1.0" or something similar. This does the same thing as pressing the button on the original website, but this time you get to decide what gets sent. You can either retype the form data that you just got or put the POST command at the top of the text file you created and use >out.txt to use the file for input. Make sure there are a couple of lines after the POST command or it won't send.

An important note: there is usually a referer field in the HTTP header that should probably not get changed. If whatever you're submitting to a script that checks the referer and requires that the referer be a certain page (so people can't post from their own websites), then it needs to be what it was when you got it.

That's not a big deal of course, but it is a vital exploration of the protocol that defines how a server sends webpages and a browser requests and sends data. It is definitely recommended that you read up on some of the syntax of HTTP protocol, as well as POP3 and SMTP, which we'll be looking at shortly.

Netcat is great for exploration, but it can also serve practical uses such as checking your POP3 (port 110) e-mail. If you got a college like mine where connecting to your e-mail account requires no encryption, then you can simply connect to their POP3 server and, with the right syntax, login. Typical login looks like this:  
Pass <password>  
Login <username>

To check for e-mail, supply the word "list" on a new line. It will return the number of e-

mails you currently have as well as their sizes. Use "ret <e-mail number>" to get the e-mail.

SMTP (port 25) is similar, and for brevity's sake, it's up to you to discover syntax. I will tell you that to send e-mail to a domain outside of your business or school, you will probably have to login using an encryption method of sorts. You can make your POP3 client connect to localhost and let netcat listen on port 25 to get the login syntax if you must (this is also a good way to spoof the From: address in an e-mail).

Netcat can do numerous more things. The things that I have listed can help you if you need to check on what data one of your forms is sending, allowing you into your e-mail account when the webclient or your POP3 client is not working, and getting the source to pesky websites. Think your network's safe? You can also port scan it with Netcat to ensure yourself that unnecessary ports are blocked. On the flip side, Netcat can be used to port scan computers and/or networks to find vulnerabilities and it can be set up to be a nasty backdoor into a computer using the right command-line switches (see documentation). Now, this backdoor can either hurt or help you. There are many PERL scripts included with some versions that will allow the computer running Netcat to act as a proxy or even an IRC server. Or... you could run Netcat so that you can log in to your or someone else's computer and have cmd.exe run as soon as you connect.

In sum, get to know Netcat as well as many of the other great utilities out there. Learn the protocols and intricacies that allow the Internet to run and never quit asking questions.

#### Additional Information

Netcat was originally written by \*Hobbit\* for \*nix and was ported over to NT by Ward Pond. More information can be found in various places on the web, as well as the readme file included in most zip files. Use this powerful tool to learn and to educate others.

For more information on HTTP, POP3 and SMTP, read RFCs 1521, 1225, and 822 respectively.

# The Lantronix SCS 1620: An Unpublicized Gold Mine



by JK

This article is a simple no-nonsense run-down of the defaults and specifications of the Lantronix SCS 1620. It is used all over the place, including one of the nation's biggest chains of banks, as well as in several universities. It is surprisingly common to come across systems that have been put on a network (especially headless ones) and not configured at all. Hopefully, administrators who use these devices will realize that with the publicly available information below, their network could be penetrated easily, and subsequently computers that hold important financial information could be compromised. No one wants to see their bank account emptied as a result of negligent administration.

The SCS 1620 from Lantronix is a very cool device. It has 16 RS-232 serial ports on the back so you can control devices (primarily computers) with ease. Beyond that, it is a pizza box shaped RedHat Linux box with a 128 mb memory card, a two row LCD on the front, an optional modem module for dialup access, a 10/100 ethernet port to put it on the network, a terminal interface direct COMM access, and a PCT18 port to connect to the Lantronix PCT18 power manager.

The default banner is simply "SCS 1620". The default communication parameters for the terminal and device ports are as follows: 9600 baud, 8 data bits, 1 stop parity, No parity, Xon/Xoff flow control, port type of DCE. The modem ports' default parameters for the modem port are the same, except with a baud rate of 38400 and RTS/CTS flow control. The power manager port (PCT18) has the same defaults as the terminal and device ports, except the port type is DTE. The device and PCT18 ports can be configured for baud rates of 2400-115.2k baud, and as DTE or DCE.

By default, the only user that can log in is "sysadmin" (default password "PASS"). Once inside, you can change various settings or go into what they call root mode (simply a shell) by typing bash. From there you can SU and the default password is "root". As sysadmin or root, you can write perl scripts. So admins, when you take the SCS 1620

out of the box, don't just plug it into the network and be glad it works. Configure it (type "setup"). If properly configured however, the SCS 1620 offers excellent security and incredible functionality.

If you happen to be inside one of these boxes for whatever reason, here is a list of commands to try out (the obvious ones have no explanation, just google it!).

```

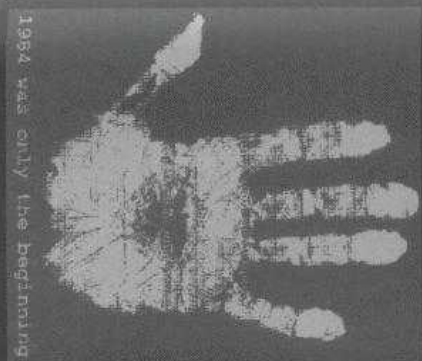
alias0
alias1
alias2
alias3
alias4
alias5
alias6
alias7
alias8
alias9
alias10
alias11
alias12
alias13
alias14
alias15
alias16
alias17
alias18
alias19
alias20
alias21
alias22
alias23
alias24
alias25
alias26
alias27
alias28
alias29
alias30
alias31
alias32
alias33
alias34
alias35
alias36
alias37
alias38
alias39
alias40
alias41
alias42
alias43
alias44
alias45
alias46
alias47
alias48
alias49
alias50
alias51
alias52
alias53
alias54
alias55
alias56
alias57
alias58
alias59
alias60
alias61
alias62
alias63
alias64
alias65
alias66
alias67
alias68
alias69
alias70
alias71
alias72
alias73
alias74
alias75
alias76
alias77
alias78
alias79
alias80
alias81
alias82
alias83
alias84
alias85
alias86
alias87
alias88
alias89
alias90
alias91
alias92
alias93
alias94
alias95
alias96
alias97
alias98
alias99
alias100
alias101
alias102
alias103
alias104
alias105
alias106
alias107
alias108
alias109
alias110
alias111
alias112
alias113
alias114
alias115
alias116
alias117
alias118
alias119
alias120
alias121
alias122
alias123
alias124
alias125
alias126
alias127
alias128
alias129
alias130
alias131
alias132
alias133
alias134
alias135
alias136
alias137
alias138
alias139
alias140
alias141
alias142
alias143
alias144
alias145
alias146
alias147
alias148
alias149
alias150
alias151
alias152
alias153
alias154
alias155
alias156
alias157
alias158
alias159
alias160
alias161
alias162
alias163
alias164
alias165
alias166
alias167
alias168
alias169
alias170
alias171
alias172
alias173
alias174
alias175
alias176
alias177
alias178
alias179
alias180
alias181
alias182
alias183
alias184
alias185
alias186
alias187
alias188
alias189
alias190
alias191
alias192
alias193
alias194
alias195
alias196
alias197
alias198
alias199
alias200
alias201
alias202
alias203
alias204
alias205
alias206
alias207
alias208
alias209
alias210
alias211
alias212
alias213
alias214
alias215
alias216
alias217
alias218
alias219
alias220
alias221
alias222
alias223
alias224
alias225
alias226
alias227
alias228
alias229
alias230
alias231
alias232
alias233
alias234
alias235
alias236
alias237
alias238
alias239
alias240
alias241
alias242
alias243
alias244
alias245
alias246
alias247
alias248
alias249
alias250
alias251
alias252
alias253
alias254
alias255
alias256
alias257
alias258
alias259
alias260
alias261
alias262
alias263
alias264
alias265
alias266
alias267
alias268
alias269
alias270
alias271
alias272
alias273
alias274
alias275
alias276
alias277
alias278
alias279
alias280
alias281
alias282
alias283
alias284
alias285
alias286
alias287
alias288
alias289
alias290
alias291
alias292
alias293
alias294
alias295
alias296
alias297
alias298
alias299
alias300
alias301
alias302
alias303
alias304
alias305
alias306
alias307
alias308
alias309
alias310
alias311
alias312
alias313
alias314
alias315
alias316
alias317
alias318
alias319
alias320
alias321
alias322
alias323
alias324
alias325
alias326
alias327
alias328
alias329
alias330
alias331
alias332
alias333
alias334
alias335
alias336
alias337
alias338
alias339
alias340
alias341
alias342
alias343
alias344
alias345
alias346
alias347
alias348
alias349
alias350
alias351
alias352
alias353
alias354
alias355
alias356
alias357
alias358
alias359
alias360
alias361
alias362
alias363
alias364
alias365
alias366
alias367
alias368
alias369
alias370
alias371
alias372
alias373
alias374
alias375
alias376
alias377
alias378
alias379
alias380
alias381
alias382
alias383
alias384
alias385
alias386
alias387
alias388
alias389
alias390
alias391
alias392
alias393
alias394
alias395
alias396
alias397
alias398
alias399
alias400
alias401
alias402
alias403
alias404
alias405
alias406
alias407
alias408
alias409
alias410
alias411
alias412
alias413
alias414
alias415
alias416
alias417
alias418
alias419
alias420
alias421
alias422
alias423
alias424
alias425
alias426
alias427
alias428
alias429
alias430
alias431
alias432
alias433
alias434
alias435
alias436
alias437
alias438
alias439
alias440
alias441
alias442
alias443
alias444
alias445
alias446
alias447
alias448
alias449
alias450
alias451
alias452
alias453
alias454
alias455
alias456
alias457
alias458
alias459
alias460
alias461
alias462
alias463
alias464
alias465
alias466
alias467
alias468
alias469
alias470
alias471
alias472
alias473
alias474
alias475
alias476
alias477
alias478
alias479
alias480
alias481
alias482
alias483
alias484
alias485
alias486
alias487
alias488
alias489
alias490
alias491
alias492
alias493
alias494
alias495
alias496
alias497
alias498
alias499
alias500
alias501
alias502
alias503
alias504
alias505
alias506
alias507
alias508
alias509
alias510
alias511
alias512
alias513
alias514
alias515
alias516
alias517
alias518
alias519
alias520
alias521
alias522
alias523
alias524
alias525
alias526
alias527
alias528
alias529
alias530
alias531
alias532
alias533
alias534
alias535
alias536
alias537
alias538
alias539
alias540
alias541
alias542
alias543
alias544
alias545
alias546
alias547
alias548
alias549
alias550
alias551
alias552
alias553
alias554
alias555
alias556
alias557
alias558
alias559
alias560
alias561
alias562
alias563
alias564
alias565
alias566
alias567
alias568
alias569
alias570
alias571
alias572
alias573
alias574
alias575
alias576
alias577
alias578
alias579
alias580
alias581
alias582
alias583
alias584
alias585
alias586
alias587
alias588
alias589
alias590
alias591
alias592
alias593
alias594
alias595
alias596
alias597
alias598
alias599
alias600
alias601
alias602
alias603
alias604
alias605
alias606
alias607
alias608
alias609
alias610
alias611
alias612
alias613
alias614
alias615
alias616
alias617
alias618
alias619
alias620
alias621
alias622
alias623
alias624
alias625
alias626
alias627
alias628
alias629
alias630
alias631
alias632
alias633
alias634
alias635
alias636
alias637
alias638
alias639
alias640
alias641
alias642
alias643
alias644
alias645
alias646
alias647
alias648
alias649
alias650
alias651
alias652
alias653
alias654
alias655
alias656
alias657
alias658
alias659
alias660
alias661
alias662
alias663
alias664
alias665
alias666
alias667
alias668
alias669
alias670
alias671
alias672
alias673
alias674
alias675
alias676
alias677
alias678
alias679
alias680
alias681
alias682
alias683
alias684
alias685
alias686
alias687
alias688
alias689
alias690
alias691
alias692
alias693
alias694
alias695
alias696
alias697
alias698
alias699
alias700
alias701
alias702
alias703
alias704
alias705
alias706
alias707
alias708
alias709
alias710
alias711
alias712
alias713
alias714
alias715
alias716
alias717
alias718
alias719
alias720
alias721
alias722
alias723
alias724
alias725
alias726
alias727
alias728
alias729
alias730
alias731
alias732
alias733
alias734
alias735
alias736
alias737
alias738
alias739
alias740
alias741
alias742
alias743
alias744
alias745
alias746
alias747
alias748
alias749
alias750
alias751
alias752
alias753
alias754
alias755
alias756
alias757
alias758
alias759
alias760
alias761
alias762
alias763
alias764
alias765
alias766
alias767
alias768
alias769
alias770
alias771
alias772
alias773
alias774
alias775
alias776
alias777
alias778
alias779
alias780
alias781
alias782
alias783
alias784
alias785
alias786
alias787
alias788
alias789
alias790
alias791
alias792
alias793
alias794
alias795
alias796
alias797
alias798
alias799
alias800
alias801
alias802
alias803
alias804
alias805
alias806
alias807
alias808
alias809
alias810
alias811
alias812
alias813
alias814
alias815
alias816
alias817
alias818
alias819
alias820
alias821
alias822
alias823
alias824
alias825
alias826
alias827
alias828
alias829
alias830
alias831
alias832
alias833
alias834
alias835
alias836
alias837
alias838
alias839
alias840
alias841
alias842
alias843
alias844
alias845
alias846
alias847
alias848
alias849
alias850
alias851
alias852
alias853
alias854
alias855
alias856
alias857
alias858
alias859
alias860
alias861
alias862
alias863
alias864
alias865
alias866
alias867
alias868
alias869
alias870
alias871
alias872
alias873
alias874
alias875
alias876
alias877
alias878
alias879
alias880
alias881
alias882
alias883
alias884
alias885
alias886
alias887
alias888
alias889
alias890
alias891
alias892
alias893
alias894
alias895
alias896
alias897
alias898
alias899
alias900
alias901
alias902
alias903
alias904
alias905
alias906
alias907
alias908
alias909
alias910
alias911
alias912
alias913
alias914
alias915
alias916
alias917
alias918
alias919
alias920
alias921
alias922
alias923
alias924
alias925
alias926
alias927
alias928
alias929
alias930
alias931
alias932
alias933
alias934
alias935
alias936
alias937
alias938
alias939
alias940
alias941
alias942
alias943
alias944
alias945
alias946
alias947
alias948
alias949
alias950
alias951
alias952
alias953
alias954
alias955
alias956
alias957
alias958
alias959
alias960
alias961
alias962
alias963
alias964
alias965
alias966
alias967
alias968
alias969
alias970
alias971
alias972
alias973
alias974
alias975
alias976
alias977
alias978
alias979
alias980
alias981
alias982
alias983
alias984
alias985
alias986
alias987
alias988
alias989
alias990
alias991
alias992
alias993
alias994
alias995
alias996
alias997
alias998
alias999
alias1000

```

You didn't think we'd let our 20th anniversary go by without introducing a brand new t-shirt, did you?



Now you can help us celebrate this momentous event by sporting one of these spiffy gray shirts with colorful artwork on the front and back that instantly identifies you as someone with a clue as to what's REALLY going on.




**1984 was only the beginning.**  
 \$18 per shirt, sizes S,M,L,XL,XXL,XXXL  
 2600  
 P.O. Box 752  
 Middle Island, NY  
 11953 USA  
 or order straight from our online store at <https://store.2600.com>






**Alaska**  
 Summit flight: 500 seats for 2007.  
**Arizona**  
 Adolpho: 100,000 seats for 2007.  
 Arizona: 100,000 seats for 2007.  
 Arizona: 100,000 seats for 2007.  
**California**  
 California: 100,000 seats for 2007.  
 California: 100,000 seats for 2007.  
**Colorado**  
 Colorado: 100,000 seats for 2007.  
 Colorado: 100,000 seats for 2007.  
**Florida**  
 Florida: 100,000 seats for 2007.  
 Florida: 100,000 seats for 2007.  
**Georgia**  
 Georgia: 100,000 seats for 2007.  
 Georgia: 100,000 seats for 2007.  
**Illinois**  
 Illinois: 100,000 seats for 2007.  
 Illinois: 100,000 seats for 2007.  
**Indiana**  
 Indiana: 100,000 seats for 2007.  
 Indiana: 100,000 seats for 2007.  
**Iowa**  
 Iowa: 100,000 seats for 2007.  
 Iowa: 100,000 seats for 2007.  
**Kansas**  
 Kansas: 100,000 seats for 2007.  
 Kansas: 100,000 seats for 2007.  
**Michigan**  
 Michigan: 100,000 seats for 2007.  
 Michigan: 100,000 seats for 2007.  
**Minnesota**  
 Minnesota: 100,000 seats for 2007.  
 Minnesota: 100,000 seats for 2007.  
**Missouri**  
 Missouri: 100,000 seats for 2007.  
 Missouri: 100,000 seats for 2007.  
**Nebraska**  
 Nebraska: 100,000 seats for 2007.  
 Nebraska: 100,000 seats for 2007.  
**Nevada**  
 Nevada: 100,000 seats for 2007.  
 Nevada: 100,000 seats for 2007.  
**New York**  
 New York: 100,000 seats for 2007.  
 New York: 100,000 seats for 2007.  
**North Carolina**  
 North Carolina: 100,000 seats for 2007.  
 North Carolina: 100,000 seats for 2007.  
**Ohio**  
 Ohio: 100,000 seats for 2007.  
 Ohio: 100,000 seats for 2007.  
**Oklahoma**  
 Oklahoma: 100,000 seats for 2007.  
 Oklahoma: 100,000 seats for 2007.  
**Pennsylvania**  
 Pennsylvania: 100,000 seats for 2007.  
 Pennsylvania: 100,000 seats for 2007.  
**Rhode Island**  
 Rhode Island: 100,000 seats for 2007.  
 Rhode Island: 100,000 seats for 2007.  
**Texas**  
 Texas: 100,000 seats for 2007.  
 Texas: 100,000 seats for 2007.  
**Virginia**  
 Virginia: 100,000 seats for 2007.  
 Virginia: 100,000 seats for 2007.  
**Washington**  
 Washington: 100,000 seats for 2007.  
 Washington: 100,000 seats for 2007.  
**West Virginia**  
 West Virginia: 100,000 seats for 2007.  
 West Virginia: 100,000 seats for 2007.  
**Wisconsin**  
 Wisconsin: 100,000 seats for 2007.  
 Wisconsin: 100,000 seats for 2007.  
**Wyoming**  
 Wyoming: 100,000 seats for 2007.  
 Wyoming: 100,000 seats for 2007.


# Payphones From All Around



**Ethiopia.** Not very many payphones to be found in this country but here's one of them in Addis Ababa.



**India.** On Elephanta Island in Mumbai, some citizens' partners sponsored this phone but not enough to dampen its brilliant yellow spirit.



**Sen Lankas.** Found in Seyruya, this booth holds the mounting from a previous tenant.



**Photos by Tom Mele**

Come and visit our website and see our vast array of payphone photos that we've compiled! <http://www.2600.com>